# MOHAN BABU UNIVERSITY

Sree Sainath Nagar, Tirupati – 517 102

DREAM. BELIEVE. ACHIEVE

## SCHOOL OF COMPUTING

## M.Tech. Computer Science and Engineering (Cyber Security)

**CURRICULUM AND SYLLABUS**

*(From 2022-23 Admitted Students)*

**FULLY FLEXIBLE CHOICE BASED CREDIT SYSTEM (FFCBCS)**

# MOHAN BABU UNIVERSITY

## Vision

To rise as one of the greatest hubs of innovation and entrepreneurship in the country, wherein students empower themselves with the best of knowledge, unleash their potential to the fullest, and soar high to attain a brighter future for themselves and the nation.

## Mission

- To provide relevant knowledge founded on the spirit of curiosity, compassion, courage and commitment.
- To uphold novelle wings of leadership and excellence under expert mentors who guide students towards wisdom and knowledge.
- To create a dynamic learning environment that empowers learners with the right blend of passion and purpose to build a glorious tomorrow.

## DEPARTMENT OF DATA SCIENCE

### VISION

To become a nationally recognized quality education center in the domain of Computer Science and Cyber Security through teaching, training, learning, research and consultancy.

### MISSION

- The Department strives to produce high quality information technologists and Cyber security Professionals by disseminating knowledge through contemporary curriculum, competent faculty and adopting effective teaching-learning methodologies.
- Igniting passion among students for research and innovation by exposing them to real time systems and problems
- Developing technical and life skills in diverse community of students with modern training methods to solve problems in Software Industry.
- Inculcating values to practice engineering in adherence to code of ethics in multicultural and multi discipline teams.

# M.Tech. COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

## PROGRAM EDUCATIONAL OBJECTIVES

After few years of graduation, the graduates of CSE (CS) will:

**PEO1.** Carry out research in the frontier areas of Computer Science and Engineering & Cyber Security and develop innovative solutions to meet the opportunities and challenges in the society. **(Research)**

**PEO2.** Employed in academia, software development, Government organizations or would have established startup companies. **(Career)**

**PEO3.** Demonstrate effective communication and leadership skills, gain knowledge of contemporary and global issues and strive for continuous learning and practice their profession with high regard to legal and ethical responsibilities. **(Professionalism, Intellectual Curiosity)**

## PROGRAM OUTCOMES

On successful completion of the Program, the graduates of M.Tech. CSE (CS) Program will be able to:

**PO1.** Demonstrate knowledge with ability to select, learn and apply appropriate techniques, skills and modern engineering tools to solve engineering problems appropriate to the relevant Computer Science and Engineering and Cyber Security discipline. **(Knowledge, Skills, Tools)**

**PO2.** Analyze engineering problems critically, conceptualize, design, implement, evaluate and manage potential solutions to contribute to the development of scientific/technological solutions in the context of relevant Computer Science and Engineering and Cyber Security discipline. **(Analyze, Design, Implement, Evaluate, Manage)**

**PO3.** Apply contextual knowledge, ethical principles and norms of engineering practice to assess societal, environmental, health, safety, legal and cultural issues pertaining to Computer Science and Engineering and Cyber Security problems. **(Professionalism, Society, Environment)**

**PO4.** Independently carry out research/investigation and development work to solve practical Computer Science and Engineering and Cyber Security problems. **(Research)**

**PO5.** Function effectively as an individual and in a team to possess knowledge and recognize opportunities for career progression and research in the Computer Science and Engineering and Cyber Security discipline. **(Individual and Team Work)**

**PO6.** Communicate effectively in professional practice through verbal and written formats. **(Communication)**

**PO7.** Recognize the need for self-motivated pursuit of knowledge to show commitment and competence in the broadest context of technological change. **(Self-Learning)**

# M.Tech. COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

## Basket Wise - Credit Distribution

| S. No. | Basket | Credits<br>(Min.- Max.) |
|---|---|---|
| 1 | SCHOOL CORE | 31 - 34 |
| 2 | PROGRAM CORE | 21 – 24 |
| 3 | PROGRAM ELECTIVE | 12 - 18 |
| 4 | UNIVERSITY ELECTIVE | 6 |
| | **TOTAL CREDITS** | **Min. 70** |

# School Core (31 - 34 Credits)

| Course Code | Title of the Course | Lecture | Tutorial | Practical | Project based Learning | Credits | Pre-requisite |
|---|---|---|---|---|---|---|---|
| | | L | T | P | S | C | |
| 22CB201001 | Number Theory and Cryptography | 3 | - | - | - | 3 | - |
| 22EE201001 | Research Methodology | 3 | - | - | - | 3 | - |
| 22EE201002 | INNOVATION AND INTELLECTUAL PROPERTY RIGHTS | 2 | - | - | - | 2 | - |
| 22CB211001 | Internship | - | - | - | - | 2 | - |
| 22CB209001 | Project Work Phase-I | - | - | - | - | 10 | - |
| 22CB210001 | Project Work Phase-II | - | - | - | - | 14 | - |
| **Mandatory Non-Credit Courses (Min. 4 Credits) Earned Credits will not be considered for CGPA** | | | | | | | |
| 22AI207601 | Statistics with R | 2 | - | - | - | 2 | - |
| 22LG207601 | Technical Report Writing | 2 | - | - | - | 2 | - |
| 22MG207601 | Project Management | 2 | - | - | - | 2 | - |
| 22MG207602 | Essentials of Business Etiquettes | 2 | - | - | - | 2 | - |

# Program Core (21 - 24 Credits)

| Course Code | Title of the Course | Lecture | Tutorial | Practical | Project based Learning | Credits | Pre-requisite/ Anti-requisite |
|---|---|---|---|---|---|---|---|
| | | L | T | P | S | C | |
| 22CB201002 | Cyber Crime and Laws | 3 | - | - | - | 3 | - |
| 22CB201003 | Cyber Risk Management and Disaster Recovery | 3 | - | - | - | 3 | |
| 22CB201004 | Secure Software Engineering | 3 | - | - | - | 3 | |
| 22CB201005 | Digital Watermarking and Steganography | 3 | - | - | - | 3 | 22CB202002 |
| 22CB202001 | Advanced Computer Networks | 3 | - | 3 | - | 4.5 | - |
| 22CB202002 | Applied Cryptography | 3 | - | 3 | - | 4.5 | - |
| 22CB202003 | Computer System Security | 3 | - | 3 | - | 4.5 | 22CB202001 |
| 22CB202004 | Network Forensics | 3 | - | 3 | - | 4.5 | 22CB202002 |
| 22CB201006 | Cloud & IoT Security | 3 | - | - | - | 3 | |
| 22CB201007 | Ethical Hacking | 3 | - | - | - | 3 | |

## Program Elective (12 - 18 Credits)

| Course Code | Knowledge Area | Title of the Course | Lecture | Tutorial | Practical | Project based Learning | Credits | Pre-requisite/ Anti-requisite |
|---|---|---|---|---|---|---|---|---|
| | | | L | T | P | S | C | |
| 22CB202005 | Data Security | Digital Forensics | 3 | - | 3 | - | 4.5 | 22CB202004 |
| 22CB201008 | | Machine Learning for Cyber Security | 3 | - | - | - | 3 | 22CB202001 |
| 22CB202006 | | Database and Web Security | 3 | - | 3 | - | 4.5 | 22CB202002 |
| 22CB201009 | Connection Security | Wireless and Mobile Network Security | 3 | - | - | - | 3 | 22CB202003 |
| 22CB202007 | | Network Anomaly Detection System | 3 | - | 3 | - | 4.5 | 22CB202001 |
| 22CB201010 | | Industry Critical Infrastructure Security | 3 | - | - | - | 3 | 22CB202001 |
| 22CB202008 | Organizational Security | Network Operations and Security | 3 | - | 3 | - | 4.5 | 22CB202001 |
| 22CB201011 | | Information Warfare | 3 | - | - | - | 3 | 22CB202001 |
| 22CB201012 | | Computer Security Audit and Assurance | 3 | - | - | - | 3 | |

## University Elective (6 Credits)

| Course Code | Title of the Course | Lecture | Tutorial | Practical | Project based Learning | Credits | Pre-requisite |
|---|---|---|---|---|---|---|---|
| | | L | T | P | S | C | |
| 22AI201701 | Business Analytics | 3 | - | - | - | 3 | - |
| 22CM201701 | Cost Management of Engineering Projects | 3 | - | - | - | 3 | - |
| 22CE201701 | Disaster Management | 3 | - | - | - | 3 | - |
| 22SS201701 | Value Education | 3 | - | - | - | 3 | - |
| 22SS201702 | Pedagogy Studies | 3 | - | - | - | 3 | - |
| 22LG201701 | Personality Development through Life Enlightenment Skills | 3 | - | - | - | 3 | - |

**Note:**

1. If any student has chosen a course or equivalent course from the above list in their regular curriculum then, he/she is not eligible to opt the same course/s under University Elective.

2. The student can choose courses from other disciplines offered across the schools of MBU satisfying the pre-requisite other than the above list.

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201001** | **NUMBER THEORY AND CRYPTOGRAPHY** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This Course Provides a Detailed Discussion on Number Theory, Algebraic Structures, Probability Theory, Coding Theory and Pseudorandom Number for understanding Methods and Algorithms in Cryptography.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Demonstrate Knowledge on algorithms such as the Euclidean algorithm, the Chinese Remainder algorithm, binary powering for Number Theory

**CO2**. Analyze Algebraic Structures for cryptography using symmetric key and public-key algorithms.

**CO3**. Demonstrate knowledge on Probability Theory and Coding Theory in Network security

**CO4**. Apply Pseudorandom Number Generation in Cryptography

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| CO1 | 3 | | | - | - | - | - |
| CO2 | 3 | 3 | | - | - | - | - |
| CO3 | 3 | - | - | - | - | - | - |
| CO4 | 3 | 3 | 3 | - | - | - | - |
| Course Correlation Mapping | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module I: Number Theory (09 Periods)**

Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm- Fermat's theorem - Euler totient function - Euler's theorem, Congruence: Definition – Basic properties of congruence's - Residue classes - Chinese remainder theorem

**Module II: Algebraic Structures** **(09 P*eriods*)**

Groups – Cyclic groups, Co-sets, modulo groups - Primitive roots – Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – $GF(p^n)$, $GF(2^n)$ - Classification - Structure of finite fields, Lattice, Lattice as Algebraic system, sub lattices, some special lattices***.***

**Module III: Probability Theory** **(09 Periods)**

Introduction – Concepts of Probability - Conditional Probability - Bayes' Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process Markov Chain

**Module IV: Coding Theory** **(09 Periods)**

Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding–Hamming codes - Hadamard Code - Goppa codes.

**Module V: Pseudorandom Number Generation** **(09 P*eriods*)**

Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum-Blum-Shub Generator – Security of the BBSGenerator.

**Total Periods: *45***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1. The Euclidean algorithm has been known for over 2000 years and has always been a favorite among number theorists. After these many years, there is now a potential competitor, invented by J. Stein in 1961. Stein's algorithms is as follows: Determine gcd(A, B) with A, B Ú 1.
   STEP 1 Set A1 = A, B1 = B, C1 = 1
   STEP 2 For n > 1, (1) If An = Bn, stop. gcd(A, B) = AnCn
   (2) If An and Bn are both even, set An+1 = An/2, Bn+1 = Bn/2,
   Cn+1 = 2Cn
   (3) If An is even and Bn is odd, set An+1 = An/2, Bn+1 = Bn,
   Cn +1 = Cn
   (4) If An is odd and Bn is even, set An+1 = An, Bn+1 = Bn/2,
   Cn +1 = Cn
   (5) If An and Bn are both odd, set An+1 = An - Bn , Bn+1 =
   min (Bn, An), Cn+1 = Cn
   Continue to step n + 1.
   a. To get a feel for the two algorithms, compute gcd(6150, 704) using both the Euclidean and Stein's algorithm.
   b. What is the apparent advantage of Stein's algorithm over the Euclidean algorithm?
2. A common formulation of the Chinese remainder theorem (CRT) is as follows: Let $m_1$, ….., $m_k$ be integers that are pairwise relatively prime for 1 … i, j … k, and i ≠ j. Define M to be the product of all the mi>s. Let $a_1$, ….., $a_k$ be integers. Then the set of congruence's:
   x = $a_1$(mod m1)
   x = a2(mod m2)
   .
   .

.

$x = a_k(\text{mod } mk)$

has a unique solution modulo M. Show that the theorem stated in this form is true.

3. For the group Sn of all permutations of n distinct symbols,
   a. what is the number of elements in Sn?
   b. show that Sn is not abelian for n >2.
4. Determine the multiplicative inverse of $x^2 + 1$ in $GF(2^3)$ with $m(x) = x^3 + x - 1$ .

**TEXT BOOKS:**

1. William Stallings, "*Cryptography and Network Security - Principles and Practice", 7th Edition*, Pearson Publications, 2017.
2. Donald Childers and Scott Miller, "Probability and Random Processes", Second Edition, Elsevier,2012

**REFERENCE BOOKS:**

1. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
2. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
3. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.

**WEB RESOURCES:**

1. https://courseware.cutm.ac.in/courses/number-theory-cryptography/
2. https://nptel.ac.in/courses/106103015
3. https://www.youtube.com/watch?v=AbjhsGnKEtE

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22EE201001** | **RESEARCH METHODOLOGY** | 3 | - | - | - | 3 |

**Pre-Requisite** --

**Anti-Requisite** --

**Co-Requisite** --

**COURSE DESCRIPTION:**
The course is developed for the students' to understand the underlying concepts of research methodology and a systematic approach for carrying out research in the domain of interest. The course is emphasised on developing skills to recognise and reflect the strength and limitation of different types of research; formulation of the research hypothesis and its systematic testing methods. The course also emphasises on interpreting the findings and research articulating skills along with the ethics of research.

**COURSE OUTCOMES:** *After successful completion of the course, students will be able to:*

**CO1.** Demonstrate the underlying concepts of research methodology, types of research and the systematic research process.

**CO2.** Demonstrate the philosophy of research design, types of research design and develop skills for a good research design.

**CO3.** Demonstrate the philosophy of formulation of research problem, methods of data collection, review of literature and formulation of working hypothesis.

**CO4.** Analyse the data and parametric tests for testing the hypothesis.

**CO5.** Interpret the findings and research articulating skills along with the ethics of research.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| **CO1** | - | - | - | 3 | - | - |
| **CO2** | - | - | - | 3 | - | - |
| **CO3** | - | - | - | 3 | - | - |
| **CO4** | - | - | - | 3 | - | - |
| **CO5** | - | - | - | - | 3 | - |
| **Course Correlation Mapping** | **-** | **-** | **-** | **3** | **3** | **-** |

*Correlation Levels: 3: High; 2: Medium; 1: Low*

## COURSE CONTENT

### Module 1: INTRODUCTION TO RESEARCH METHODOLOGY (08 Periods)

Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, and Significance of Research, Research Methods versus Methodology, Research and Scientific Method, Research Process, Criteria of Good Research.

### Module 2: RESEARCH DESIGN (08 Periods)

Research design—Basic Principles, Need of research design, Features of good design, Important concepts relating to research design, Different research designs, Basic principles of experimental designs, Developing a research plan.

### Module 3: RESEARCH FORMULATION (08 Periods)

Defining and formulating the research problem - Selecting the problem - Necessity of defining the problem - Importance of literature review in defining a problem – Data collection – Primary and secondary sources; Critical literature review – Identifying gap areas from literature review; Hypothesis— Types of hypothesis, Development of working hypothesis.

### Module 4: ANALYSIS OF DATA AND HYPOTHESIS TESTING (14 Periods)

**Quantitative Tools**: Testing and Significance of Measures of Central Tendency, Dispersion; correlation, Principles of least squares—Regression; Errors-Mean Square error, Mean absolute error, Mena absolute percentage errors.

**Testing of Hypothesis**: Hypothesis Testing Procedure, Types of errors, Parametric testing (t, z and F), Chi-Square Test as a Test of Goodness of Fit; Normal Distribution- Properties of Normal Distribution; Analysis of Variance.

### Module 5: INTERPRETATION AND REPORT WRITING (07 Periods)

**Interpretation**: Meaning of interpretation; Techniques of interpretation; Precautions in Interpretation.

**Report Writing** –Significance, Different Steps, Layout, Types of reports, Mechanics of Writing a Research Report, Precautions in Writing Reports; Research ethics—Plagiarism, Citation and acknowledgement.

**Total Periods: *45***

## EXPERIENTIAL LEARNING

1. Should conduct a survey based on a hypothesis, analyze the data collected and draw the inferences from the data.
2. Should review the literature on the given topic and should identify the scope/gaps in the literature and develop a research hypothesis.
3. Should study a case, formulate the hypothesis and identify an appropriate testing technique for the hypothesis.
4. Study an article and submit a report on the inferences and should interpret the findings of the article.

## RESOURCES

### TEXT BOOKS:

1. C.R. Kothari, Research Methodology: Methods and Techniques, New Age International Publishers, 2nd revised edition, New Delhi, 2004.
2. Garg, B.L., Karadia, R., Agarwal, F. and Agarwal, *An introduction to Research Methodology*, RBSA Publishers, 2002.

### REFERENCE BOOKS:

1. R. Panneerselvam, Research Methodology, PHI learning Pvt. Ltd., 2009.
2. Singh, Yogesh Kumar. *Fundamental of research methodology and statistics*. New Age International, 2006.

### VIDEO LECTURES:

1. https://nptel.ac.in/courses/121106007
2. https://onlinecourses.nptel.ac.in/noc22_ge08/preview
3. https://www.youtube.com/watch?v=VK-rnA3-41c

### WEB RESOURCES:

1. https://www.scribbr.com/category/methodology/
2. https://leverageedu.com/blog/research-design/
3. https://prothesiswriter.com/blog/how-to-formulate-research-problem
4. https://www.formpl.us/blog/hypothesis-testing
5. https://www.datapine.com/blog/data-interpretation-methods-benefits-problems/
6. https://leverageedu.com/blog/report-writing/

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22EE201002** | **INNOVATION AND INTELLECTUAL PROPERTY RIGHTS** | 2 | - | - | - | 2 |

**Pre-Requisite** --

**Anti-Requisite** --

**Co-Requisite** --

**COURSE DESCRIPTION:**

The course is designed to provide comprehensive knowledge to the students regarding the general principles of intellectual property rights, Concept and Theories, Criticisms of Intellectual Property Rights, International Regime Relating to IPR. The course provides an awareness on how to protect ones unique creation, claim ownership, knowledge of what falls under the purview of someone's rights and what doesn't, and safeguard their creations and gain a competitive edge over the peers.

**COURSE OUTCOMES:** *After successful completion of the course, students will be able to:*

**CO1.** Understand the need and the concepts of intellectual property right and avenues for filling intellectual property rights.

**CO2.** Understand the legislative practices and protocols for acquisition of trademark and the judicial consequences for violating laws of trademark protection.

**CO3.** Understand the legislative practices and protocols for acquisition of copyrights and the judicial consequences for violating laws of copyrights protection.

**CO4.** Understand the fundamentals of patent laws, legislative practices and protocols for acquisition of trade secrets and the judicial consequences for violating laws of trade secrets protection.

**CO5.** Understand the latest developments and amendments in protection and filling of intellectual rights at international level.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | -- | -- | -- | 2 | 3 | 3 |
| **CO2** | 3 | -- | 2 | -- | 2 | 3 | 3 |
| **CO3** | 3 | -- | 2 | -- | 2 | 2 | 3 |
| **CO4** | 3 | -- | 2 | -- | 2 | 2 | 3 |
| **CO5** | 3 | -- | 2 | -- | 2 | 2 | 3 |
| **Course Correlation Mapping** | **3** | **--** | **2** | **--** | **2** | **3** | **3** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: INTRODUCTION TO INTELLECTUAL PROPERTY RIGHTS (06 Periods)**

Introduction and the need for intellectual property rights (IPR); types of intellectual property- Design, Geographical Indication; International organizations, agencies and treaties.

**Module 2: TRADEMARKS (06 Periods)**

Introduction to trademark, Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting and evaluating trade mark, trade mark registration processes.

**Module 3: LAW OF COPYRIGHTS (06 Periods)**

Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right registration, notice of copy right, international copy right law.

**Law of patents:** Foundation of patent law, patent searching process, ownership rights and transfer.

**Module 4: TRADE SECRETS (06 Periods)**

Trade secrete law, determination of trade secrete status, liability for misappropriations of trade secrets, and protection for submission, trade secrete litigation.

**Unfair competition:** Misappropriation right of publicity, false advertising.

**Module 5: NEW DEVELOPMENT OF INTELLECTUAL PROPERTY (06 Periods)**

New developments in: trade mark law, copy right law, patent law, intellectual property audits. International overview on intellectual property; international - trade mark law, copy right law, international patent law, international development in trade secrets law.

**Total Periods: 30**

***Topics for self-study are provided in the lesson plan.***

## EXPERIENTIAL LEARNING

1. Should conduct a survey based on the real scenario, where IPR is misused or unethically used and present an article.
2. Prepare an article on the registration processes of IPR practically (copy right/trade mark/ patents).
3. Should study a case of conflict on trademarks/patents and should produce an article mentioning the circumstances and remedial measures.
4. Prepare an article on the latest development in the international intellectual property rights.

## RESOURCES

### TEXT BOOKS:

1. Deborah, E. Bouchoux, *Intellectual property: The law of Trademarks, Copyright, Patents, and Trade Secrets,* Cengage learning, 4th Edition, 2013.
2. Prabuddha Ganguli, *Intellectual property right - Unleashing the knowledge economy*, Tata McGraw Hill Publishing Company Ltd.

### REFERENCE BOOKS:

1. Neeraj P., & Khusdeep D. Intellectual Property Rights. India, IN: PHI learning Private Limited. 1st Edition 2019.
2. Nithyananda, K V. Intellectual Property Rights: Protection and Management. India, IN: Cengage Learning India Private Limited. 2019

### VIDEO LECTURES:

1. https://nptel.ac.in/courses/110105139

### WEB RESOURCES:

1. Subramanian, N., & Sundararaman, M. (2018). *Intellectual Property Rights – An Overview*. Retrieved from http://www.bdu.ac.in/cells/ipr/docs/ipr-eng-ebook.pdf
2. World Intellectual Property Organisation. (2004). *WIPO Intellectual property Handbook*. Retrieved from https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf
3. Cell for IPR Promotion and Management (http://cipam.gov.in/)
4. World Intellectual Property Organisation (https://www.wipo.int/about-ip/en/)
5. Office of the Controller General of Patents, Designs & Trademarks (http://www.ipindia.nic.in/)

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| 22CB211001 | INTERNSHIP | - | - | - | - | 2 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Expose students to the industrial environment; Create competent professionals for the industry; sharpen the real time technical / managerial skills required at the job; Gain professional experience and understand engineer‷s responsibilities and ethics; Familiarize with latest equipment, materials and technologies; Gain exposure to technical report writing; Gain exposure to corporate working culture.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Analyze latest equipment, materials and technologies that are used in industry to solve complex engineering problems following relevant standards, codes, policies and regulations.

**CO2.** Analyze safety, health, societal, environmental, sustainability, economical and managerial factors considered in industry in solving complex engineering problems.

**CO3.** Perform individually or in a team besides communicating effectively in written, oral and graphical forms on practicing engineering.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| CO1 | 3 | 3 | - | 3 | 3 | - | - |
| CO2 | - | 3 | - | - | - | 3 | 3 |
| CO3 | - | - | - | - | - | - | - |
| Course Correlation Mapping | 3 | 3 | - | 3 | 3 | 3 | 3 |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

# SCHOOL CORE

| Course Code | Course Title | L T P S C |
|---|---|---|
| **22CB209001** | **PROJECT WORK PHASE-I** | - - - - 10 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Identification of topic for the project work; Literature survey; Collection of preliminary data; Identification of implementation tools and methodologies; Performing critical study and analysis of the problem identified; submitting a Report.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Apply contextual knowledge to identify specific domain in cyber security and allied areas of discipline.

**CO2.** Conduct literature review, analyze, cognize and comprehend the extracted information to recognize the current status of research pertinent to the chosen domain.

**CO3.** Select appropriate tools, techniques and resources for implementation of project work.

**CO4.** Function effectively as an individual to recognize the opportunities in the chosen domain of interest

**CO5.** Write and present a technical report/document to present the findings on the chosen problem.

**CO6.** Engage lifelong learning for development of technical competence in the field of cyber security.

### CO-PO Mapping Table:

| **Course Outcomes** | | **Program Outcomes** | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO2** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO3** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO4** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **CO5** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **CO6** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **Course Correlation Mapping** | **3** | **2** | **2** | **2** | **2** | **2** | **3** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

# SCHOOL CORE

| Course Code | Course Title | L T P S C |
|---|---|---|
| **22CB210001** | **PROJECT WORK PHASE-II** | - - - - 14 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Time and cost analysis; undertaking practical investigations of project work; implementation; analysis of results; validation and report writing.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Create/Design algorithms and software to undertake practical investigations of project work, analyze and interpret results.

**CO2.** Utilize appropriate tools, techniques and resources for implementation of project work.

**CO3.** Function effectively as an individual to recognize the opportunities in the chosen domain of interest

**CO4.** Write and present a technical report/document to present the findings on the chosen problem.

**CO5.** Engage lifelong learning for development of technical competence in the field of cyber security.

## CO-PO Mapping Table:

| **Course Outcomes** | | **Program Outcomes** | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO2** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO3** | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| **CO4** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **CO5** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **CO6** | 3 | 2 | 2 | 2 | 2 | 2 | - |
| **Course Correlation Mapping** | **3** | **2** | **2** | **2** | **2** | **2** | **3** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22AI207601** | **STATISTICS WITH R** | 2 | - | - | - | 2 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course introduces the basic concepts of statistics using R language. The course also deals with various types of sampling methods and its impact in the scope of inference through the computation of confidence intervals. The topics covered in the course also includes descriptive statistics, marginal and conditional distribution, statistical transformations, chi-squared test and ANOVA.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Import, manage, manipulate, structure data files and visualize data using R programming.

**CO2.** Identify trends and patterns in data using Marginal, Conditional distributions andStatistical transformations.

**CO3.** Analyse data using sampling and probability distribution methods and compute confidence intervals for statistical inference.

**CO4.** Apply chi-squared goodness-of-fit test, Pearson's $\chi$ 2-statistic and ANOVA to investigatethe distribution of data.

### CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| **CO1** | 3 | 2 | - | - | - | - |
| **CO2** | 3 | 2 | - | - | - | - |
| **CO3** | 2 | 2 | - | - | - | - |
| **CO4** | 3 | 2 | - | - | - | - |
| **Course Correlation Mapping** | 3 | 2 | - | - | - | - |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: INTRODUCTION** ***(05 Periods)***

Data, R's command line, Variables, Functions, The workspace, External packages, Data sets, Data vectors, Functions, Numeric summaries, Categorical data.

**Module 2: BIVARIATE AND MULTIVARIATE DATA** ***(07 Periods)***

Lists, Data frames, Paired data, Correlation, Trends, Transformations, Bivariate categorical data, Measures of association, Two-way tables, Marginal distributions, Conditional distributions, Graphical summaries, Multivariate data - Data frames, Applying a function overa collection, Using external data, Lattice graphics, Grouping, Statistical transformations.

**Module 3 POPULATIONS** ***(06 Periods)***

Populations, Discrete random variables, Random values generation, Sampling, Families of distributions, Central limit theorem, Statistical Inference - Significance tests, Estimation, Confidence intervals, Bayesian analysis.

**Module 4 CONFIDENCE INTERVALS** ***(06 Periods)***

Confidence intervals for a population proportion, p - population mean, other confidence intervals, Confidence intervals for differences, Confidence intervals for the median, Significance test - Significance test for a population proportion, Significance test for the mean (t-tests), Significance tests and confidence intervals, Significance tests for the median.

**Module 5 GOODNESS OF FIT** ***(06 Periods)***

The chi-squared goodness-of-fit test, The multinomial distribution, Pearson's $\chi$ 2-statistic, chi-squared test of independence and homogeneity, Goodness-of-fit tests for continuous distributions, ANOVA - One-way ANOVA, Using *lm* for ANOVA.

***Total Periods: 30***

## EXPERIENTIAL LEARNING

1. The data set baby boom (Using R) contains data on the births of 44 children in a one-day period at a Brisbane, Australia, hospital. Compute the skew of the wt variable, which records birth weight. Is this variable reasonably symmetric or skewed? The variable running. time records the time after midnight of each birth. The command diff(running.time) records the differences or inter-arrival times. Is thisvariable skewed?
2. An elevator can safely hold 3, 500 pounds. A sign in the elevator limits the passenger count to 15. If the adult population has a mean weight of 180 pounds with a 25-pound standard deviation, how unusual would it be, if the central limit theorem applied, thatan elevator holding 15 people would be carrying more than 3, 500 pounds?
3. The data set MLB Attend (Using R) contains attendance data for Major League Baseball between the years 1969 and 2000. Use lm to perform a t-test on attendance for the two levels of league. Is the difference in mean attendance significant? Compare your results to those provided by t-test.

## RESOURCES

### TEXT BOOKS:

1. John Verzani, *Using R for Introductory Statistics*, CRC Press, 2nd Edition, 2014.
2. Sudha G Purohit, Sharad D Gore, Shailaja R Deshmukh, *Statistics Using R*, Narosa Publishing house, 2nd Edition, 2021.

### REFERENCE BOOKS:

1. Francisco Juretig, *R Statistics Cookbook*, Packt Publishing, 1st Edition, 2019.
2. Prabhanjan N. Tattar, Suresh Ramaiah, B. G. Manjunath, *A Course in Statistics with R*, Wiley, 2018.

### VIDEO LECTURES:

1. https://onlinecourses.nptel.ac.in/noc21_ma76/preview
2. https://onlinecourses.nptel.ac.in/noc19_ma33/preview
3. https://youtu.be/WbKiJe5OkUU?list=PLFW6lRTa1g83jjpIOte7RuEYCwOJa-6Gz
4. https://youtu.be/svDAkvh6utM?list=PLFW6lRTa1g83jjpIOte7RuEYCwOJa-6Gz
5. https://nptel.ac.in/courses/111104120

### WEB RESOURCES:

1. https://www.geeksforgeeks.org/r-statistics/
2. https://www.geeksforgeeks.org/r-programming-exercises-practice-questions-and- solutions/
3. https://www.w3schools.com/r/r_stat_intro.asp
4. https://www.w3schools.com/r/r_stat_intro.asp
5. https://statsandr.com/blog/descriptive-statistics-in-r/

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22LG207601** | **TECHNICAL REPORT WRITING** | 2 | - | - | - | 2 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course deals with preparing effective technical documents for both written and digital media, with particular emphasis on technical memos, problem-solving and decision-making reports, and organizational, product-support, and technical-information webs.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Demonstrate knowledge of Technical Report Writing and structures with a scientific attitude.

**CO2.** Analyze the process of writing in preparing effective reports.

**CO3.** Demonstrate styles of writing for Publication in a Scientific Journal.

**CO4.** Apply the process of referencing and editing techniques for effective communication in written documents.

**CO5.** Analyze the strategies in the technical report presentation.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** |
| **CO1** | - | - | - | - | 3 | - |
| **CO2** | - | - | - | - | 3 | - |
| **CO3** | - | - | - | - | 3 | - |
| **CO4** | - | - | - | - | 3 | - |
| **CO5** | - | - | - | - | 3 | - |
| **Course Correlation Mapping** | **-** | **-** | **-** | **-** | **3** | **-** |

*Correlation Levels: 3: High; 2: Medium; 1: Low*

## COURSE CONTENT

**Module 1: INTRODUCTION TO TECHNICAL REPORT WRITING** ***(06 Periods)***

Concepts of Technical Report, Types of Reports, Planning Technical Report Writing, Components of a Technical Report, Report Writing in Science and Technology, Selecting and Preparing a Title, Language Use in Report Writing.

**Module 2: PROCESSOF WRITING** ***(06 Periods)***

Writing the 'Introduction', Writing the 'Materials and Methods, Writing the Findings/Results, Writing the 'Discussion', Preparing and using "Tables'.

**Module 3: STYLE OF WRITING** ***(06 Periods)***

Preparing and using Effective 'Graphs', Citing and Arranging References-I, Citing and Arranging References –II, Writing for Publication in a Scientific Journal.

**Module 4: REFERENCING** ***(06 Periods)***

Literature citations, Introductory remarks on literature citations, Reasons for literature citations, Bibliographical data according to ISO standards, Citations in the text, Copyright, and copyright laws, the text of the Technical Report, Using a word processing and desktop publishing (DTP) systems, Document or page layout, hints on editing Typographic details, Cross-references.

**Module 5: PRESENTATION** ***(06 Periods)***

Presentation with appropriate pointing, Dealing with intermediate questions, Review and analysis of the presentation, Rhetoric tips from A to Z.

***Total Periods: 30***

## EXPERIENTIAL LEARNING

1. Prepare a report on technologies of modern times that enriched the originality of research works and their impacts on society concerning plagiarism.
2. Make PowerPoint presentations on the various style of writing academic reports.
3. Error-free Reports are so important for successful communication and sharing of information. Prepare a detailed chart on proofreading techniques to make a report effective and error-free.
4. Design a logo for a company and write down the copy-right laws for that.
5. Read research articles from any international journal of science and technology and differentiate research writing from other academic and non-academic writings.
6. Write an organizational memo Include a heading, introduction, and summary at the beginning of your memo, and present the details of your discussion in a logical order. Use headings and topic or main-idea sentences to clarify the organization.
7. Prepare an appraisal report on the staff performance of your company.
8. Prepare a PowerPoint presentation on the annual performance report of a company.

9. Critically review and write a report on any one of the recently released products.
10. Read the newspaper and write a detailed report about the content coverage and analyse the factors for the popularity of the newspaper.

## RESOURCES

### TEXT BOOKS:

1. RC Sharma and Krishna Mohan, "*Business Correspondence and Report Writing*", McGraw-Hill Publishing, 3rd Edition, 2005 (reprint).
2. Patrick Forsyth, "*How to Write Reports and Proposals*", The Sunday Times, Kogan Page, New Delhi, Revised 2nd Edition, 2010.

### REFERENCE BOOKS:

1. John Seely, *"The Oxford Writing & Speaking"*, Oxford University Press, Indian Edition
2. Anne Eisenberg, "*A Beginner's Guide to Technical Communication*", McGraw-Hill Education (India) Private Limited, New Delhi, 2013.

### VIDEO LECTURES:

1. https://vimeo.com/143714818
2. https://digitalmedia.sheffield.ac.uk/media/002.+The+Anatomy+of+a+Technical+Report/1_u8wntcge

### WEB RESOURCES:

1. http://www.resumania.com/arcindex.html
2. http://www.aresearchguide.com/writing-a-technical-report.htm
3. http://www.sussex.ac.uk/ei/internal/forstudents/engineeringdesign/studyguides/tec report writing

## SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22MG207601** | **PROJECT MANAGEMENT** | 2 | - | - | - | 2 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite**

**COURSE DESCRIPTION:** To understand the importance of decision-making while implementing any project and interpret and discuss the results of qualitative and quantitative analysis

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

| | |
|---|---|
| **CO1** | Understand the basic introduction to project management |
| **CO2** | Apply the methods of project identification and selection. |
| **CO3** | Understand project allocation methods and evaluation. |
| **CO4** | Analyse the techniques for project time, review, and cost |
| **CO5** | Understand the factors of risk and quality of a project. |

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** |
| **CO1** | 2 | 1 | 2 | 1 | - | - |
| **CO2** | 1 | 1 | 2 | 2 | - | |
| **CO3** | 2 | 2 | 1 | 2 | 1 | - |
| **CO4** | 3 | 1 | 2 | 2 | 1 | - |
| **CO5** | 2 | 2 | 1 | 2 | 1 | 1 |
| **Course Correlation Mapping** | **2** | **2** | **2** | **2** | **1** | **1** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

### COURSE CONTENT

**Module 1: Introduction** ***(05 Periods)***

Concept of project management, project definition and key features of projects, project life cycle phases, typical project management issues, basic project activities

**Module 2: Project Identification and Selection** ***(06 Periods)***

Identification and screening (brainstorming, strength and weakness in the system, environmental opportunities and threats), Project evaluation methods- Payback period, Net present value, Internal rate of return and project evaluation under uncertainty.

**Module 3: Project Resource Management** ***(07 Periods)***

Scheduling resources, resource allocation methods, project crashing and resource leveling, working of systems, design of systems, project work system design, project execution plan, project procedure manual project control system, planning scheduling and monitoring

**Module 4: Time and Cost Management** ***(05 Periods)***

Time Management-Network diagram, forward and backward pass, critical path, PERT and CPM, AOA and AON methods, tools for project network, Cost management-earned value method

**Module 5: Risk and Quality Management** ***(07 Periods)***

Risk identification, types of risk, risk checklist, risk management tactics, risk mitigation and contingency planning, risk register, communication management, Quality assurance and quality control, quality audit, methods of enhancing quality

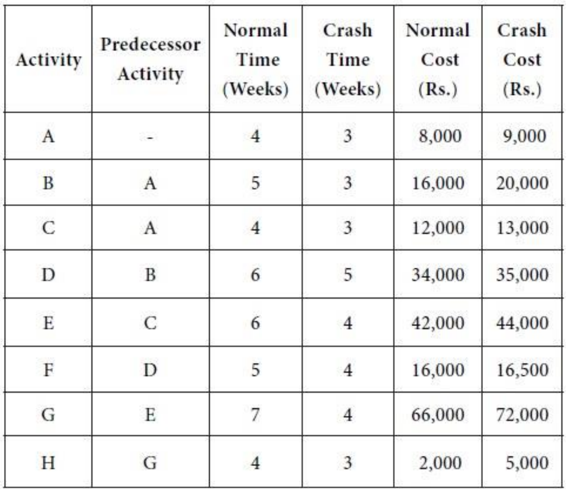
***Total Periods: 30***

## EXPERIENTIAL LEARNING

1. Refer to any video lecture on project evaluation methods and give a brief seminar using PPT

2. Select any company wherein you will get the details of activities and time and draw the project network diagram and submit a report.

3.



| Activity | Predecessor Activity | Normal Time (Weeks) | Crash Time (Weeks) | Normal Cost (Rs.) | Crash Cost (Rs.) |
|---|---|---|---|---|---|
| A | - | 4 | 3 | 8,000 | 9,000 |
| B | A | 5 | 3 | 16,000 | 20,000 |
| C | A | 4 | 3 | 12,000 | 13,000 |
| D | B | 6 | 5 | 34,000 | 35,000 |
| E | C | 6 | 4 | 42,000 | 44,000 |
| F | D | 5 | 4 | 16,000 | 16,500 |
| G | E | 7 | 4 | 66,000 | 72,000 |
| H | G | 4 | 3 | 2,000 | 5,000 |

Determine a crashing scheme for the above project so that the total project time is reduced by 3 weeks

4. Collect any case study that discusses the process of probability calculation of success of the project and submit a report

## RESOURCES

### TEXT BOOKS:

1. R.Panneerselvam and P.Senthil Kumar (2013), Project Management, PHI Learning Private Limited.
2. Prasanna Chandra (2014), Projects: Planning, Analysis, Selection, Financing, implementation, and Review.

### REFERENCE BOOKS:

1. A Guide to the Project Management Body of Knowledge: (PMBOK Guide) by Project Management Institute, 2013.
2. Gopala Krishnan & Rama Murthy, A Text book of Project Management, McMillan India.
3. S. Choudhary (2004), Project Management, Tata McGraw Hill Publication.

### VIDEO LECTURES:

1. https://onlinecourses.nptel.ac.in/noc19_mg30/preview
2. https://archive.nptel.ac.in/courses/110/104/110104073/

### WEB RESOURCES:

1. https://www.pmi.org/about/learn-about-pmi/what-is-project-management
2. https://www.manage.gov.in/studymaterial/PM.pdf

# SCHOOL CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22MG207602** | **ESSENTIALS OF BUSINESS ETIQUETTES** | 2 | - | - | - | 2 |

**Pre-Requisite**

**Anti-Requisite**

**Co-Requisite** -

**COURSE DESCRIPTION:** This course is designed for learners who desire to improve their Business etiquette and professionalism.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** learn the principles of business etiquettes and professional behavior

**CO2.** understand the etiquettes for making business correspondence effective

**CO3.** Develop awareness of dining and multicultural etiquettes

**CO4.** Demonstrate an understanding of professionalism in terms of workplace behaviors and workplace relationships.

**CO5.** Understand attitudes and behaviors consistent with standard workplace expectations.

**CO-PO Mapping Table:**

| **Course Outcomes** | **Program Outcomes** | | | | | |
|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** |
| **CO1** | 1 | 1 | - | - | - | 1 |
| **CO2** | 1 | 1 | 2 | 1 | - | 1 |
| **CO3** | 2 | - | 2 | - | 1 | - |
| **CO4** | 1 | 2 | - | 1 | - | - |
| **CO5** | 1 | 2 | 1 | - | - | - |
| **Course Correlation Mapping** | **2** | **2** | **2** | **1** | **1** | **1** |

*Correlation Levels: 3: High; 2: Medium; 1: Low*

## COURSE CONTENT

**Module 1: Business Etiquettes- An Overview** ***(06 Periods)***

Significance of Business Etiquettes in 21st Century- Professional Advantage; Need and Importance of Professionalism; Workplace Etiquette: Etiquette for Personal Contact- Personal Appearance, Gestures, Postures, Facial Expressions, Eye-contact, Space distancing

**Module 2: Communication Skills** ***(06 Periods)***

Understanding Human Communication, Constitutive Processes of Communication, Language as a tool of communication, Barriers to Effective communication, and Strategies to Overcome the Barriers.

**Module 3: Teamwork and Leadership Skills** ***(06 Periods)***

Concept of Teams; Building effective teams; Concept of Leadership and honing Leadership skills. Personality: Meaning & Definition, Determinants of Personality, Personality Traits, Personality and Organisational Behaviour Motivation: Nature & Importance, Herzberg's Two Factor theory, Maslow's Need Hierarchy theory, Alderfer's ERG theory

**Module 4: Interview Skills** ***(06 Periods)***

Interview Skills: in-depth perspectives, Interviewer and Interviewee, Before, During and After the Interview, Tips for Success. Meeting Etiquette: Managing a Meeting-Meeting agenda, Minute taking,; Duties of the chairperson and secretary; Effective Meeting Strategies - Preparing for the meeting, Conducting the meeting, Evaluating the meeting

**Module 5: Decision-Making and Problem-Solving Skills** ***(06 Periods)***

Decision-Making and Problem-Solving Skills: Meaning, Types and Models, Group and Ethical Decision-Making, Problems and Dilemmas in application of these skills. Conflict Management: Conflict - Definition, Nature, Types and Causes; Methods of Conflict Resolution.

***Total Periods:30***

## EXPERIENTIAL LEARNING

### LIST OF EXPERIMENTS:

1. Collect the case studies related to successful leaders and their traits.
2. Conduct a mock interview showcasing interview skills.
3. The case studies will be collected as Assignments and the same will be evaluated.

## RESOURCES

### TEXT BOOKS:

1. Barbara Pachter, Marjorie Brody. Complete Business Etiquette Handbook. Prentice Hall, 2015.
2. Mahanand, Anand. English for Academic and Professional Skills. Delhi: McGraw, 2013. Print.

### REFERENCE BOOKS:

1. Pease, Allan and Barbara Pease. The Definitive Book of Body Language. New Delhi: Manjul Publishing House, 2005.
2. Rani, D Sudha, TVS Reddy, D Ravi, and AS Jyotsna. A Workbook on English Grammar and Composition. Delhi: McGraw, 2016.

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=NqlfZOPMqjA
2. http://www.nitttrc.edu.in/nptel/courses/video/109104107/L24.html

### WEB RESOURCES:

1. http://elibrary.gci.edu.np/bitstream/123456789/685/1/BM-783%20The%20Essential%20Guide%20to%20Business%20Etiquette%20by%20Lillian%20H.%20Chaney%2C%20Jeanette%20S.%20Martin.pdf
2. The Essentials of Business Etiquette: How to Greet, Eat, and Tweet Your Way to Success by Barbara Pachter (Ebook) - Read free for 30 days (everand.com)

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201002** | **CYBER CRIME AND LAWS** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on Cyber Crimes and Indian IT Act; Cyber Offenses; Tools and Methods used in Cyber Crime; Phishing ad Identity Theft; Indian and Global Perspective on Cyber Crimes and Cyber Security; Organizational Implications on Cyber Security; IPR Issues; Cyber

Crime and Terrorism; Cyber Crime Illustrations

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Demonstrate knowledge in Cyber security, Cybercrimes and its related laws in Indian and Global Act.

**CO2.** Analyze the legal perspectives and laws related to cybercrimes in Indian context.

**CO3.** Apply security and privacy methods in development of modern applications and in organizations to protect people and to prevent cybercrimes.

**CO4.** Solve Cyber security issues using privacy policies and Use antivirus tools to minimize the impact of cyber threats.

**CO5.** Apply security standards for the implementation of Cyber Security and laws.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | | | - | - | - | - |
| **CO2** | 3 | 3 | | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | 3 | 3 | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **3** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: INTRODUCTION TO CYBER CRIMES AND OFFENSES** ***(09 Periods)***

**Cyber Crimes:** Introduction, Definition, Origin, Cybercrime and information security, Cyber criminals, Classifications of cybercrimes, The legal perspectives and Indian perspective, Cybercrime and Indian ITA 2000, Global perspective on cybercrimes.
**Cyber Offenses:** Introduction, Criminals planning on attacks, Social engineering, Cyber stalking, Cyber cafe and crimes, Botnets.

**Module 2: TOOLS AND METHODS USED IN CYBER CRIME AND PHISHING AND IDENTITY THEFT** ***(09 Periods)***

Introduction, Proxy servers and Anonymizers, Phishing, Password cracking, Key loggers and Spywares, Virus, Worms and Ransomware, Trojan horses and Backdoors, Steganography, DoS and DDoS attacks.
**Phishing and Identity Theft:** Introduction, Phishing, Identity Theft (ID Theft).

**Module 3 CYBER CRIMES AND CYBER SECURITY-LEGAL PERSPECTIVES** ***(08 Periods)***

Introduction, Cyber laws in Indian context, The Indian IT act, Challenges to Indian law and Cybercrime scenario in India, Consequences of not addressing the weakness in IT act, Digital signatures and the Indian IT Act, Cyber Crime and Punishment, Cyber law, Technology and Students in India scenario.

**Module 4 CYBER SECURITY-ORGANIZATIONAL IMPLICATIONS** ***(10 Periods)***

Introduction, Web threats for organizations – evils and perils, Security and privacy implications from cloud computing, Social Media Marketing-Security risks and Perils for organizations, Social computing and associated challenges for organizations, Protecting people's privacy in organization, Organizational guidelines for internet usage, Safe computing and Usage policy, Incident handling and Best practices.

**Module 5 CYBER CRIME AND TERRORISMAND ILLUSTRATIONS** ***(09 Periods)***

**Cyber Crime & Terrorism:** Introduction, Intellectual property in the cyber space, The ethical dimension of cybercrimes, The psychology, Mindset and skills of hackers and cyber criminals, Sociology of cyber criminals, Information warfare.
**Cyber Crime Illustrations:** Indian banks lose millions of rupees, Justice vs. Justice, Parliament attack, The Indian case of online gambling, Bank and credit card related frauds, Purchasing goods and services scam, Nigerian 419 scam.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. The Cyber Security Risks on Social Media – Learn from Case Studies: https://www.rswebsols.com/tutorials/internet/cyber-security-risks-social-media
2. SIX automates key cybersecurity tasks to actively protect itself against social media threats: https://www.hootsuite.com/resources/six-group-case-study
3. Important Cyber Law Case Studies : https://www.cyberralegalservices.com/detail-casestudies.php

## RESOURCES

### TEXT BOOKS:

1 Nina Gobole and SunitBelapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India, 2011.

### REFERENCE BOOKS:

1. Prashant Mali, Cyber Law and Cyber Crimes, Snow White Publications Pvt. Ltd., 2013.
2. Cyber Security and Cyber Laws Alfred Basta and et al Cengage Learning India 2018

### VIDEO LECTURES:

1. Learn Cyber Security | Cyber Security Training: https://www.youtube.com/watch?v=PlHnamdwGmw
2. Cyber Security For Beginners: https://www.youtube.com/watch?v=4RE4d23tDFw

### WEB RESOURCES:

1. Introduction to Cybersecurity: https://study.com/academy/course/computer-science-110-introduction-to-cybersecurity.html
2. Types of Cyber Crimes: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/
3. Cyber Security: Spam, Scams, Frauds and Identity Theft: https://mediasmarts.ca/digital-media-literacy/digital-issues/cyber-security/cyber-security-spam-scams-frauds-identity-theft

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201003** | **CYBER RISK MANAGEMENT AND DISASTER RECOVERY** | 3 | - | - | - | 3 |

| | |
|---|---|
| **Pre-Requisite** | - |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** This course provides a detailed discussion on Concepts of Incident Response: Planning, Detection and Decision Making & Organizing and Preparing the CSIRT, Response Strategies and Recovery and Maintenance, Disaster Recovery: Preparation and Implementation, Operation and Maintenance

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the planning process of Incident Response in Risk Management

**CO2.** Apply Incident Detection, Decision Making, and CSIRT techniques for Intrusion Detection and Prevention.

**CO3.** Apply Response Strategies and perform Recovery and Maintenance tasks

**CO4.** Analyze the preparation and implementation methodology for Disaster Recovery.

**CO5.** Apply the Operation and Maintenance approaches for Disaster Recovery.

### CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | 3 | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

## COURSE CONTENT

**Module 1: Incident Response: Planning** ***(11 Periods)***

The IR Planning Process, Developing the Incident Response Policy, Incident Response Planning, Information for attack success end case, Reaction, The CCDC, Assembling and Maintaining the Final IR Plan.

**Module 2: Detection and Decision Making & Organizing and Preparing the CSIRT** ***(10 Periods)***

***Detection and Decision Making:*** Detecting Incidents, Technical Details: Rootkits, Intrusion Detection and Prevention Systems, Technical Details: Processes and Services, Technical Details: Ports and Port Scanning, Incident Decision Making.
***Organizing and Preparing the CSIRT :*** Building the CSIRT, A Sample Generic Policy and High-Level Procedures for Contingency Plans, Outsourcing Incident Response.

**Module 3 Response Strategies and *Recovery and Maintenance*** ***(11 Periods)***

***Response Strategies:*** IR Response Strategies, The Cuckoo's Egg, Incident Containment and Eradication Strategies for Specific Attacks, Egghead, Automated IR Response Systems.
***Recovery and Maintenance:*** Recovery, Maintenance, Sample Impact Analysis, Incident Forensics, Technical Details, Discovery and Anti-Forensics.

**Module 4 Disaster Recovery: Preparation and Implementation** ***(10 Periods)***

Introduction, Disaster Classifications, Forming the Disaster Recovery Team, Disaster Recovery Planning Functions, Information Technology Contingency Planning Considerations, Sample Disaster Recovery Plans, The DR Plan

**Module 5 Disaster Recovery: Operation and Maintenance** ***(10 Periods)***

Opening Case Scenario: Dastardly Disaster Drives Dialing, Introduction, Facing Key Challenges, Preparation: Training the DR Team and the Users, Disaster Response Phase, Recovery Phase, Resumption Phase, Restoration Phase

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Creating a control system Human Machine Interface (HMI)
2. Python scripts for log analysis and reverse engineering
3. Understanding basic firewall rule configuration (Authentication, Authorization, and Accounting)
4. Vulnerability assessment and tools

## RESOURCES

### TEXT BOOKS:

1. Herbert Mattord, Michael Whitman, Cengage "Principles of Incident Response & Disaster Recovery", 2nd Edition, Cengage Learning, 2013

### REFERENCE BOOKS:

1. M.E. Sharpe. Waugh, William L. Jr. "Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management" Armonk, New York ,2000.

2. Andy Jones, Debi Ashenden "Risk Management for Computer Security: Protecting Your Network & Information Assets" , 1st Edition, Butterworth

3. Andreas Von Grebmer "Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security", 2008, Books On Demand Gmbh.

**VIDEO LECTURES:**

1. Disaster risk: Hazards X Exposure X Vulnerability: **https://youtu.be/UtufcbtXKMk**
2. Risk Perception and Disaster Risk Preparedness: **https://youtu.be/JmQWPaXPofk**

**WEB RESOURCES:**

1. Disaster Risk Reduction and Management: **https://www.slideshare.net/irpex/disaster-risk-reduction-and-management-28415360**
2. Disaster Risk Reduction, Disaster Risk Management and Disaster Management:: **https://www.researchgate.net/publication/264863987_Disaster_Risk_Reduction_Disaster_Risk_Management_and_Disaster_Management_Academic_Rhetoric_or_Practical_Reality**
3. Disaster Risk and Resilience : **https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/3_disaster_risk_resilience.pdf**
4. Disaster Risk Management : **https://www.bivica.org/files/desastres-contribuciones.pdf**

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201004** | **SECURE SOFTWARE ENGINEERING** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on Concepts of Software Security Engineering provides tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data. This course includes importance of security in software, requirements engineering, security principles in SDLC, security & complexity and governance & managing.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the importance of security in software

**CO2.** Applying methods to detect software security defects, SQUARE process model for requirement gathering and coding practices

**CO3.** Analyze complex software projects to describe security risks and mitigation techniques and security testing for identifying security failures.

**CO4.** Analyze research issues in code analysis techniques to improve software security.

**CO5.** Apply Governance and Managing for more secure software.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | 3 | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: IMPORTANCE OF SECURITY IN SOFTWARE** ***(10 Periods)***

***Security a Software Issue:*** Introduction, The problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of detecting software security defects early, managing secure software development.
***Secure Software:*** Introduction, Properties of Secure Software, Influencing the security properties of software, Asserting and specifying the desired security properties.

**Module 2: REQUIREMENTS ENGINEERING** ***(09 Periods)***

***Requirements Engineering for Secure Software:*** Introduction, Misuse and abuse cases, the SQUARE process Model, SQUARE sample outputs, Requirements elicitation, Requirements prioritization.

**Module 3 SECURITY PRINCIPLES IN SDLC** ***(10 Periods)***

***Secure Software Architecture and Design*:** Introduction, Software Security practices for Architecture and Design - architectural risk analysis, Software security knowledge for Architecture and Design - Security principles, Security guidelines and Attack patterns.
***Secure Coding and Testing:*** Introduction, Code analysis, Coding Practices, Software Security testing, Security testing considerations throughput the SDLC.

**Module 4 SECURITY AND COMPLEXITY** ***(08 Periods)***

***System Assembly Challenges:*** Introduction, Security failures, functional and attacker perspectives for security analysis in web services and identity management, system complexity drivers and security, Deep technical problem complexity.

**Module 5 GOVERNANCE AND MANAGING** ***(08 Periods)***

***Governance and Managing for more Secure Software:*** Introduction, Governance and security, adopting an enterprise software security framework, Defining adequate security, Risk Management framework for software security, Security and Project Management, Maturity of Practice.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Input Validation and Output Encoding
2. .NET Authentication and Authorization
3. Secure Session and State Management
4. .NET Cryptography
5. .NET Error Handling, Auditing, and Logging
6. .NET Secure File Handling
7. .NET Configuration Management and Secure Code Review

## RESOURCES

**TEXT BOOKS:**

1. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, and Nancy R. Mead,"Security Engineering: A Guide for Project Managers," Pearson Education, 2009.

**REFERENCE BOOKS:**

1. Gary McGraw, "Software Security: Building Security In," Addison
2. Mark Dowd, John McDonald and Justin Schuh, "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities," 1st Edition, Addison

3. John Viega and Gary McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way," Addison
4. G. Hoglund and G. McGraw, "Exploiting Software: How to Break Code," Addison-Wesley, 2004.

**VIDEO LECTURES:**

1. Secure Software Engineering, https://www.youtube.com/c/securesoftwareengineering
2. Secure Software Engineering : Secure Design Principles & Coding Practices https://www.youtube.com/watch?v=teLmHBPGiV8&ab_channel=NPTEL-SpecialLectureSeries

**WEB RESOURCES:**

1. Secure Software Engineering : Secure Design Principles & Coding Practices : https://youtu.be/teLmHBPGiV8
2. Essential Activities for Secure Software Development: https://www.researchgate.net/publication/340298331_Essential_Activities_for_Secure_Software_Development
3. **Understanding Software Architecture Vs. Software Security Design** : https://sopa.tulane.edu/blog/understanding-software-architecture-vs-software-security-design
4. A Governance Framework for Building Secure IT Systems : https://www.researchgate.net/publication/228404647_A_Governance_Framework_for_Building_Secure_IT_Systems

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201005** | **DIGITAL WATERMARKING AND STEGANOGRAPHY** | 3 | - | - | - | 3 |

**Pre-Requisite** Applied Cryptography (22CB202002)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on fundamentals of watermarking and steganography, Coding and Encoding, Watermarking types, Watermarking techniques, steganography approaches and applications.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Impart knowledge on digital watermarking, fundamental issues and a threat model.

**CO2.** Analyse various coding techniques and watermarking types to embed watermarks into multimedia data.

**CO3.** Apply watermarking techniques to design applications for secure data transmission.

**CO4.** Apply multimedia encryption and steganography approaches for multimedia authentication.

**CO5.** Identify various applications of watermarking and steganography.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | - | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

**COURSE CONTENT**

**Module 1: INTRODUCTION** ***(09 Periods)***

Information Hiding, Digital Watermarking and Steganography, need of watermarking, Ownership Assertion, Properties of Watermarking Systems, Fundamental Issues, Information Hiding Methods, threat model.

**Module 2: DIGITAL WATERMARKING** ***(08 Periods)***

Models of Watermarking, Basic Message Coding, Error Correction Coding Watermarking Encoding and decoding, Classification, Robust Watermarks, Fragile Watermarks, Additive Watermarks, advantage and disadvantage of watermarking.

**Module 3: DIGITAL COMMUNICATION AND PROTOCOLS** ***(10 Periods)***

Mutual Information and Channel Capacity, Spread Spectrum Watermarking, Block DCT-domain Watermarking, Watermarking with Side-Information (Dirty-paper Coding), Improved Spread Spectrum Watermarking, Affine-Resistant Watermarking, Media Specific Digital Watermarking Image Watermarking, Video Watermarking, Audio Watermarking, Watermarking for CG-models Watermarking for Binary Images Watermarking for 3D Contents Data Hiding through watermarking techniques, A Buyer-Seller Watermarking, Extensions of Watermarking Protocols, Protocols for Secure Computation.

**Module 4: WATERMARKING SECURITY AND STEGANALYSIS** ***(10 Periods)***

Cryptography and Multimedia Encryption, Multimedia Processing in the Encryption Domain, Privacy preserving Information Processing, Authentication of Multimedia (issues and challenges), Techniques for Authentication, content authentication.

Foundations of Steganography - Introduction to Steganalysis, the Building Blocks, Notation and Terminology, Steganographic Methods, Steganalysis Scenarios, Significant Steganalysis Algorithms.

**Module 5: APPLICATIONS** ***(8 Periods)***

Applications of Digital Watermarking, Broadcast Monitoring, Owner Identification, Proof of Ownership, Transaction Tracking, Applications of Steganography, Steganography for Dissidents, Steganography for Criminals.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Develop an application to embed a watermark into an Image for proof of ownership.
2. Design and develop an application to hide/extract information into/from an Image for secret data transmission.

## RESOURCES

**TEXT BOOKS:**

1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. 2nd Edition, Morgan Kaufmann Publishers, 2008.
2. Ingemar Cox, Matthew Miller, Jeffrey Bloom, and Jessica Fridrich . Digital Watermarking and Steganography, 2nd Ed, (The Morgan Kaufmann Series in Multimedia Information and Systems). (Hardcover – Nov 16, 2007)

**REFERENCE BOOKS:**

1. Frank Y. Shih. Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press.
2. Stefan Katzenbeisser, Fabien, and A.P. Petitcolas. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House.
3. Neil F. Johnson; Zoran Duric; Sushil Jajodia. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Springer. 5. Gregory Kipper. Investigator's Guide to Steganography, Auerbach Publications.

**VIDEO LECTURES:**

1. Digital Image Processing Course,

   https://www.youtube.com/watch?v=nrYpzUsfTTc&list=PLOcXTr0yn-UoYFyHWLf1qpKoj57nUsLrt&ab_channel=PROJECTTUNNEL

**WEB RESOURCES:**

1. https://www.sciencedirect.com/book/9780123725851/digital-watermarking-and-steganography
2. http://wiki.cas.mcmaster.ca/index.php/Steganography_and_Digital_Watermarking

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202001** | **ADVANCED COMPUTER NETWORKS** | 3 | - | 3 | - | 4.5 |

| | |
|---|---|
| **Pre-Requisite** | - |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** This course provides a detailed discussion and hands-on experience on computer network concepts, TCP-IP reference model, IPV6 message format, network interfaces, performance issues in Local Area and wide area networks.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the concepts behind Opportunistic, IoT and Software Defined Networking.

**CO2.** Identify different issues in Opportunistic, Social, IoT and SDN Networks.

**CO3.** Analyze various protocols proposed to handle issues related to Opportunistic, Social, IoT and SDN Networks.

**CO4.** Demonstrate about the Cellular Communications Networks and Wireless System Evolution & TCP/IP protocols.

**CO5.** Analyze performance of Cellular and Ad Hoc Networks protocols of a network.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | - | - | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | - | - | - | - | - | - |
| **CO5** | 3 | 3 | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **-** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

### Module 1: INTRODUCTION TO OPPORTUNISTIC AND SOCIAL NETWORKS *(08 Periods)*

**Opportunistic and Social Networks:** Handling Spectrum Scarcity and Disruption, Architecture of Cognitive Radio Network (CRN) and Delay Tolerant Networks (DTN), Routing in Opportunistic Mobile and Social Networks, Multicasting, Single-node, Multiple-copy, and Single-copy model, Interest-based Data Dissemination, User Interest Profile, Multi-party data transmission, System Implementation, Quality-of-Service (QoS), QoS parameters, Metrics and classification, Network QoS parameters (bandwidth, delay, etc.), System QoS parameters (reliability, capacity, etc.), Task QoS parameters (memory, CPU usage, response time, etc.), Extension QoS parameters (reputation, security, etc.).

### Module 2: IoT NETWORKS *(09 Periods)*

**IoT Networks:** Convergence of domains, Key technologies for IoT and its components, Multi-homing, Sensing, Actuation, Data Aggregation, IoT communication patterns, IoT data and its impact on communication, Characteristics of IoT networks, Protocols for IoT, NFC (Near field communication), Tactile Internet, Caching, Edge computing, Inter-dependencies, SoA, Gateways, Comparison between IoT and Web, Complexity of IoT networks, Scalability, Protocol classification, MQTT, SMQTT, CoAP, XMPP, AMQP, Wireless HART protocol and layered architecture, HART network manager, HART vs ZigBee, Cross layer QoS parameters

### Module 3 SOFTWARE DEFINED NETWORKS (SDN) *(10 Periods)*

Network Function Virtualization (NFV), Unicast and multicast routing, Fundamental graph algorithms, Modern protocols for content delivery, Video delivery using HTTP, HTTP Live Streaming, DASH, Content Delivery Networks (CDN), TVOD and SVOD, Architecting a content distribution system over IP-based networks, CDN topologies, Edge-Caching, Streaming-Splitting, Pure-Play, Operator, Satellite, Hybrid, Computer hosting and orchestration for dedicated appliances and virtualization, Robust synchronization of absolute and difference clocks, Precision time protocol, Clock synchronization in SDN, ReversePTP scheme.

### Module 4 WIRELESS NETWORKS *(10 Periods)*

Generic Characteristics, Wireless Local Area Networks and Cellular Communications Networks. TCP Performance Issues over Wireless Links, Inappropriate Reduction of Congestion Window, Throughput Loss in WLANs and Throughput Loss in Cellular Communication Systems. Improving TCP Performance over Wireless Links: Splitting TCP Connections, Snooping TCP at Base Stations, Notifying the Causes of Packet Loss, Adding Selective Acknowledgments to TCP and Comparison of Enhancement Schemes. Wireless System Evolution and TCP/IP: Trends in Cellular Communication Systems, Trends in Wireless LAN Systems, TCP/IP over Heterogeneous Wireless systems.

### Module 5 *(08 Periods)*

**Cellular and Ad Hoc Networks:** TCP Performance in Cellular Networks, Mobile IP, Impact of Mobility on TCP Performance, Approaches to Improve TCP Performance, TCP Performance in Ad Hoc Networks, Dynamic Source Routing, Impact of Mobility on TCP Performance, Approaches to Improve TCP Performance. Evolution of Optical Networks, IP over DWDM, Multiprotocol Label Switching, Multiprotocol Lambda Switching, Optical Burst Switching, Optical Packet Switching: Optical Packet Format, Congestion Resolution in Optical Packet Switches, Performance of TCP/IP over Optical Networks, Optical Packet Network End-to-End Performance, Mapping of TCP in Optical Packets, Optical Packet Design in the TCP/IP Environment.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

### LIST OF EXERCISES:

1. Basic Network commands like :ipconfig, hostname, ping, tracert, netstat.
2. Windows 2003 server installation and basic configuration.
3. DHCP server configuration.
4. DNS & HTTP, FTP server configuration.
5. Basic Routing configuration.
6. Configure RIP2, OSPF.
7. Configure EIGRP.
8. Implement Access list / NAT technology.
9. Implement WiFi configuration.
10. Implementation of Uni cast Routing Algorithm

### SOFTWARE/TOOLS:

Cisco packet tracer simulation software.

## RESOURCES

### TEXT BOOKS:

1. Opportunistic Mobile Social Networks, Jie Wu and Yunsheng Wang, CRC Press, 2015.
2. High Performance TCP/IP: Networking Concepts, Issues, and Solutions, Mahbub Hassan and Raj Jain, 1st Edition, PHI Learning, 2009.

### REFERENCE BOOKS:

1. TCP/IP Illustrated (Volume I, Volume II and Volume III), W. Richard Stevens, Addison-Wesley
2. Computer Networking: A Top-down Approach Featuring the Internet, James F. Kurose and Keith W. Ross, Addison-Wesley, 2001.

### VIDEO LECTURES:

1. Opportunistic Mobile Networks:
   https://www.youtube.com/watch?v=j1__cQien94
2. Software Defined Networks:
   https://www.digimat.in/nptel/courses/video/106105183/L43.html
3. Basics Of IoT Networking :
   https://www.youtube.com/watch?v=fByKuk2VmJc
4. Wireless Ad Hoc and Sensor Networks :
   https://www.digimat.in/nptel/courses/video/106105160/L01.html

**WEB RESOURCES:**

1. Adhoc and Wireless Sensor Networks:
   https://www.rcet.org.in/uploads/files/LectureNotes/ece/S7/EC8702-%20AWSN/Unit-I%20-EC8702-Adhoc%20and%20Wireless%20Sensor%20Networks.pdf
2. Types of IoT Networks :
   https://www.fogwing.io/types-of-iot-networks/
3. Software-Defined Networking (SDN) :
   https://www.vmware.com/topics/glossary/content/software-defined-networking.html
   https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html
4. Wireless Networks:
   https://www.tutorialspoint.com/Wireless-Networks

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202002** | **APPLIED CRYPTOGRAPHY** | 3 | - | 3 | - | 4.5 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion and hands-on experience on Cryptographic protocols and Encryption techniques for confidentiality. Mathematical derivations for symmetric and asymmetric algorithms. It also provides Hash functions for integrity and digital signature schemes for authentication.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Apply cryptographic protocols to ensure authentication in network systems.
**CO2.** Select suitable cryptographic technique to provide data security.
**CO3.** Understand the mathematical concepts of Cryptographic algorithms and provide privacy for data.
**CO4.** Apply hash functions to provide integrity mechanisms in data communication.
**CO5.** Select suitable digital signatures techniques to enhance authentication among peer-to-peer communication.

### CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | 3 | 3 | - | - | - | - |
| **CO2** | 3 | 3 | 3 | 3 | - | - | - |
| **CO3** | 3 | - | - | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | 3 | 3 | 3 | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **3** | **-** | **-** | **-** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

## COURSE CONTENT

### Module 1: FOUNDATIONS OF CRYPTOGRAPHY *(08 Periods)*

**FOUNDATIONS OF CRYPTOGRAPHY:** Steganography, Substitution ciphers and Transposition Ciphers, One Time Pads.
**Protocol Building Blocks:** Introduction to protocols, communications using symmetric Cryptography, One-Way Hash Functions, Communications Using Public-Key Cryptography, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation, **Basic Protocols**: Key Exchange, Authentication and key Exchange.

### Module 2: CRYPTOGRAPHIC TECHNIQUES *(08 Periods)*

**CRYPTOGRAPHIC TECHNIQUES:** Key Management, Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mode, Counter Mode, Choosing a Cipher Mode, Interleaving, Block Ciphers versus Stream Ciphers.

### Module 3 MATHEMATICS FOR CRYPTOGRAPHIC ALGORITHMS *(12 Periods)*

**MATHEMATICS FOR CRYPTOGRAPHIC ALGORITHMS:** Mathematical background: Information Theory, Complexity Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field,
**Data Encryption Standard** (DES), DES decryption, Security of DES, DES variants, Public Key Algorithms: RSA, Pholig-Hellman, RABIN, Elliptic Curve Cryptosystems.

### Module 4 HASH FUNCTIONS *(08 Periods)*

**HASH FUNCTIONS:** One Way Hash Functions, Snefru hash function, N- Hash, MD4, MD5, Secure Hash Algorithm (SHA), Security of SHA, One Way Hash Functions Using Symmetric Block Algorithms, Using Public-Key Algorithms, Message Authentication Codes (MAC).

### Module 5 DIGITAL SIGNATURES *(09 Periods)*

Digital Signature Algorithm (DSA), Security of DSA, Discrete Logarithm Signature Schemes, Ongchnorr-Shamir, SCHNORR authentication and signature scheme, Diffie-Hellman Key exchange, Station-to-Station Protocol, Shamir’s Three-Pass Protocol.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

### LIST OF EXERCISES:

1 Implement the following mono alphabetic Ciphers and analyze its attack resiliency.
   a. Shift Cipher
   b. Affine cipher
2. Implement the following Poly-alphabetic Ciphers and analyze its attack resiliency.
   a. Hill cipher
   b. Vigenere
3. Implement the following block cipher modes and analyze the role of Initialization Vector (IV)
   a. counter mode
   b. Output Feedback mode
4. Write a program to implement the Data Encryption Standard (DES).
5. Implement a stream cipher algorithm with running key generator.
6. Write a program to Implement RSA algorithm.
7. Write a program to find prime factors of a given large number and analyze the time complexity.

8. Write a program to determine the message digest of a given message using the SHA-1 algorithm.
9. Write a program to implement Diffie-Hellman Key Exchange mechanism.
10. Write a program to implement Digital Signature Standard.

**SOFTWARE/TOOLS:**

Software: J2SDK 1.7

- Eclipse or Net bean

Java compatible web browser

## RESOURCES

**TEXT BOOKS:**

1. Bruce Schneier, *"Applied Cryptography: Protocols, Algorithms and Source Code in C",* John Wiley and Sons, New York, 2009.
2. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 7th Edition, 2017.

**REFERENCE BOOKS:**

1. Alfred J Menezes, Paul C van Oorschot and Scott A.Vanstone, *"Handbook of Applied Cryptography"*, CRC Press, New York, 2010.
2. Wenbo Mao, *"Modern Cryptography Theory and Practice",* Pearson Education, 2004
3. Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 3rd Edition, 2005.

**VIDEO LECTURES:**

1. https://www.coursera.org/specializations/applied-crypto
2. https://www.classcentral.com/course/udacity-applied-cryptography-326
3. https://www.udacity.com/course/applied-cryptography--cs387

**WEB RESOURCES:**

1. https://wiki.openssl.org/index.php/Command_Line_Utilities
2. https://www.sslshopper.com/article-most-common-openssl-commands.html
3. https://www.cs.virginia.edu/~evans/courses/crypto-notes.pdf
4. https://teapowered.dev/assets/crypto-notes.pdf

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202003** | **COMPUTER SYSTEM SECURITY** | 3 | - | 3 | - | 4.5 |

| | |
|---|---|
| **Pre-Requisite** | Advanced Computer Networks (22CB202001) |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** Introduction to computer security; Operating System Security Models, Unix Security, Windows Security, Storage & Database Security, Wireless Network Security

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Apply cryptographic technique and network protocols for securing administration.

**CO2:** Understand security mechanisms in various operating systems.

**CO3:** Apply mechanisms for securing data and applications.

**CO4:** Analyze security mechanisms for wireless intrusion detection and prevention.

**CO5:** Apply infrastructure services for securing E-mail, web servers, DNS servers and Proxy servers.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | 3 | 3 | - | - | - | - |
| **CO2** | 3 | - | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: INTRODUCTION** **(09 Periods)**

Computer Security, Threats, Administrative Security, Overall Planning and Administration, Day to Day Administration, About the Internet, Network Protocols,

Encryption: DES, AES, RSA.

**Module 2: COMPUTER SECURITY** **(08 Periods)**

**Operating System Security Models**: Operating System Models, Classic Security Models, Reference Monitor, Trustworthy Computing, International Standards for Operating System Security.

**Unix Security:** Securing a Unix System, Place Servers into Network Zones, Authentication Processes, Limit the Number of Administrators and Privileges, Back Up the System, Security Lists.

**Windows Security:** Securing Windows Systems, Active Directory Domain Architecture.

**Module 3: Data Security** **(08 Periods)**

**Storage Security:** Storage Security Evolution, Modern Storage Security, Risk Remediation.

**Database Security:** General Database Security Concepts, Understanding Database Security Layers, Understanding Database-Level Security, Application Security, Database Backup and Recovery, Keeping servers Up to Date, Database Auditing and Monitoring.

**Module 4: WIRELESS NETWORK SECURITY** **(10 Periods)**

Radio Frequency Security Basics, Data-Link Layer Wireless Security Features, Flaws, and Threats, Wireless Vulnerabilities and Mitigations, Wireless Network Hardening Practices and Recommendations, Wireless Intrusion Detection and Prevention, Wireless Network Positioning and Secure Gateways.

**Module 5: SECURING INFRASTRUCTURE SERVICES** **(10 Periods)**

**E-Mail:** Protocols Their Vulnerabilities and Counter measures, Spam and Spam Control
**Web Servers:** Types of Attacks, Web Server Protection
**DNS Servers:** Prevent Unauthorized Zone Transfers, DNS Cache Poisoning
**Proxy Servers:** HTTP, FTP, Direct Mapping, POP3, Reverse Proxy

**Total Periods: *45***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1. a Implement DES algorithm for the given input parameters

   b Implement AES algorithm for the given input parameters

2. a Implement RSA algorithm for the given input parameters.

   b Using RSA asymmetric cryptographic algorithm demonstrate values for Private and Public Keys in cryptographic systems

3 Implement Firewall Configuration and generate Assessment-iptables using command arguments.

4. Configure and use SSH software to establish and experiment with secure connection and detect MITM attacks (impostors) with PuTTY.
5. Write a program to Demonstrate DNS Message format for resolver library routine
6. Simulate buffer overflow attack and protect against SQL injection attack.

7. Implement Brute force and dictionary attacks to generate passwords and hashes for files created in system.

8. a. Demonstrate installation and working of Intrusion detection System (IDS)using SNORT Tool

   b. Detect and record anomalous traffic and analyze Snort alert file using SNORT Tool

9. a. Configure Snort as detection engine detecting attacks based on signatures defined by rulesets.

   b. Create simple Snort rules.

10. a. Install, configure, and experiment with a honeypot to detect, capture, and analyze attacks.

    b. Create simple honeypot scenarios and alerts, and test them with test attacks

**SOFTWARE/TOOLS:**

- JAVA/PYTHON
- SNORT Tool

## RESOURCES

**TEXT BOOKS:**

1. Rick Lehtinen, " Computer Security Basics ",O'Reilly Media, Second Edition , 2006.

2. Mark Rhodes-Ousley, "Information Security ", McGraw-Hill Obsorne Media, Second Edition, 2013.

**REFERENCE BOOKS:**

1. Craighead, Geoff. High-Rise Security and Fire Life Safety. Butterworth-Heinemann, 2003.
2. Fennelly, Lawrence J. Effective Physical Security. Butterworth-Heinemann, 1997.
3. Matchett, Alan R. CCTV for Security Professionals. Butterworth-Heinemann, 2003.

**VIDEO LECTURES:**

1. Computer Systems Security, https://css.csail.mit.edu/6.858/2022/

2. Introduction to information Security, https://archive.nptel.ac.in/courses/106/106/106106129/

**WEB RESOURCES:**

1. **https://onlinecourses.nptel.ac.in/noc22_cs36/preview**
2. **https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/**
3. **https://www.csa.iisc.ac.in/~vg/teaching/SecurityLectures/**

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202004** | **NETWORK FORENSICS** | 3 | - | 3 | - | 4.5 |

| | |
|---|---|
| **Pre-Requisite** | Applied Cryptography (22CB202002) |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** Concepts in Digital and Network Evidence; Network Evidence; OSCAR; Evidence Acquisition; Traffic Analysis, Wireless Network Forensics; Network Intrusion Detection and Analysis; Forensics in Network Devices and Servers.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1** Understand the importance of network forensic principles and technical foundations.

**CO2:** Analyse the network evidences, protocols, flow analysis using network forensic tools.

**CO3:** Apply the appropriate techniques of Network forensics in wireless and IDS.

**CO4:** Acquire knowledge about the Forensics methods in Network Devices and Servers.

**CO5:** Apply network tunnelling and Malware Forensics techniques for analysing the network

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | - | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

### Module 1: Introduction (08 Periods)

**Understanding Network Forensics*:*** Concepts in Digital and Network Evidence, Challenges Relating to Network Evidence, Network Forensics Investigative Methodology (OSCAR)

***Technical Fundamentals:*** Sources of Network-Based Evidence,On the Wire in the Air, Switches, Routers, DHCP Servers, Name Servers, Authentication Servers, Network Intrusion Detection/Prevention Systems, Firewalls, Web Proxies, Application Servers, Central Log Servers, Principles of Internetworking, Internet Protocol Suite.

### Module 2: Evidence Acquisition (07 Periods)

Physical Interception, Traffic Acquisition Software, libpcap and WinPcap, The Berkeley Packet Filter (BPF) Language, tcpdump, Wireshark, tshark, dumpcap. Active Acquisition: Common Interfaces, Inspection without Access, Strategy
**Traffic Analysis:** Protocol Analysis, Packet Analysis, Flow Analysis, Higher-Layer Traffic Analysis
**Statistical Flow Analysis:** Process Overview, Sensors, Sensor Types, Sensor Software Sensor Placement, Modifying the Environment, Flow Record Export Protocols, Collection and Aggregation, Flow Record Analysis Techniques, Flow Record Analysis Tools.

### Module 3: Wireless: Network Forensics Unplugged (10 Periods)

***Wireless Networks:*** The IEEE Layer 2 Protocol Series. Wireless Access Points (WAPs), Wireless Traffic Capture and Analysis, Common Attacks, Locating Wireless Devices.
***Network Intrusion Detection and Analysis:*** Why Investigate NIDS/NIPS, Typical NIDS/NIPS Functionality, Modes of Detection, Types of NIDS/NIPSs, NIDS/NIPS Evidence Acquisition, Comprehensive Packet Logging, Snort.

### Module 4: Forensics in Network Devices and Servers (11 Periods)

***Event Log Aggregation, Correlation, and Analysis:*** Sources of Logs, Network Log Architecture, Collecting and Analyzing Evidence.
***Switches, Routers, and Firewalls:*** Switches, Why Investigate Switches, Content-Addressable Memory Table Address Resolution Protocol, Types of Switches, Switch Evidence, Routers, Why Investigate Routers, Types of Routers, Router Evidence. Firewalls-Why Investigate Firewalls, Types of Firewalls, Firewall Evidence, Logging , Local Logging Simple Network Management Protocol, syslog, Authentication, Authorization, and Accounting Logging

### Module 5:Network Tunneling and Malware Forensics (09 Periods)

***Network Tunneling :*** Tunneling for Functionality, Tunneling for Confidentiality, Covert Tunneling ,Case Study: Ann Tunnels Underground , Analysis: Protocol Statistics, DNS Analysis ,Quest for Tunneled IP Packets, Tunneled IP Packet Analysis, Tunneled TCP Segment Analysis.
***Malware Forensics:*** Trends in Malware Evolution, Botnets, Encryption and Obfuscation Distributed Command-and-Control Systems, Automatic Self-Updates, Metamorphic Network Behavior, Blending Network Activity, Fast-Flux DNS, Advanced Persistent Threat (APT)
**Network Behavior of Malware:** Propagation, Command-and-Control Communications Payload Behavior

**Total Periods:** ***45***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1. Using EmailTrackerPro demonstrate and generate the report provides an option to report the abuse of a particular email address to the administrators of the attacker and the victim networks and also contains some critical information that can be useful for forensic analysis and investigation..

2. Give demonstrate about the tools, SmartWhoIs which allows you to look up all the available information about an IP address, hostname or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information.
   find the answers:
   to these important questions:
   a) Who is the owner of the domain?
   b) When the domain was registered and what is the owner's contact information?
   c) Who is the owner of the IP address block?
3. Consider a scenario where an attacker has planted a keylogger on one of the systems in the network. Your job as an investigator is to find the following pieces of information:
   Find the infected system.
   Trace the data to the server
   Find the frequency of the data that is being sent
   Find what other information is carried besides the keystrokes
   Try to uncover the attacker
   a) Extract and reconstruct the files that have been sent to the attacker
4. Imagine you are a network forensics expert who has been tasked with analyzing the PCAP file using Wireshark.

5. Give demonstrate about the Dissecting malware on the network, Intercepting malware for fun and profit, behavior patterns and analysis.
6. Consider Decoding the Meta sploit shell, Let's start investigating the file in Wireshark to try to deduce what happened and focus on gathering the following details:
   C2 server IP
   C2 server port
   Infected system IP
   Infected system's port
   Actions performed by the attacker
   Time of the attack
   Duration of the attack
7. Consider a scenario where we have received a PCAP file for analysis and some logs from a Linux server. By analyzing the file in Wireshark, and get the packet data using Network intrusions and footprints
8. Analyze a few of the malware samples and their network behavior, based on which we will write and make use of scripts, demonstrate the Automation using Python and Scapy,  Automation through pyshark – Python's tshark, Merging and splitting PCAP data, Large-scale data capturing, collection, and indexing.

**SOFTWARE/TOOLS:**

- Software Wireshark, Metasploit, Python and Scapy.
- Operating system: Kali Linux

## RESOURCES

### TEXT BOOKS:

1. Network Forensics: Tracking Hackers through Cyberspace 1st Edition by Sherri Davidoff (Author), Jonathan Ham (Author).
2. Learning Network Forensics Paperback – Feb. 29 2016by Samir Datt (Author)

### REFERENCE BOOKS:

1. Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools, Nipun Jaswal (Author).
2. Yuri Diogenes (Author), ErdalOzkaya (Author), Cyber security – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition Paperback – Dec 31 2019

### VIDEO LECTURES:

1. Digital Forensics, https://onlinecourses.swayam2.ac.in/cec20_lb06/preview
2. Network Forensic, https://www.youtube.com/watch?v=5wLxmVorZBM&ab_channel=MotasemHamdan%7CCyberSecurity%26Tech

### WEB RESOURCES:

1. https://www.coursera.org/lecture/technical-deep-dive-with-incident-response-tools/network-forensics-with-wireshark-lDZV7
2. https://www.learnvern.com/cyber-forensics-course/network-forensics-acquisition-technique

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201006** | **CLOUD AND IoT SECURITY** | 3 | - | 3 | - | 4.5 |

**Pre-Requisite**

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Course covers the technical aspects of

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Demonstrate the knowledge on identifying, collecting and preserving digital evidence

**CO2:** Analyse the scientific principles relating to digital forensics.

**CO3:** Perform the steps included in a digital investigation from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, and the completion of legal proceedings.

**CO4:** Acquire knowledge about the Forensics methods in Digital Evidence and Data Acquisition, Duplication.

**CO5:** Apply forensic investigation on a forensic image, using various tools to recover evidence, resulting in a report documenting the investigation

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | - | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

### MODULE I Fundamentals of IoT and Cloud Computing: (10 Periods)

Evolution of Internet of Things, Enabling Technologies, IoT Architectures: oneM2M, IoT World Forum (IoTWF) and Alternative IoT models, Simplified IoT Architecture and Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem, Sensors, Actuators, Smart Objects and Connecting Smart Objects.

### MODULE II IoT Architectures and Protocols: (10 Periods)

M2M high-level ETSI architecture, IETF architecture for IoT, OGC architecture. IoT reference model: Domain model, information model, functional model, communication model. IoT reference architecture. Protocol Standardization for IoT: Efforts, M2M and WSN Protocols, SCADA and RFID Protocols. IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, LoRaWAN, Network Layer: IP versions, Constrained Nodes and Constrained Networks. Optimizing IP for IoT: From 6LoWPAN to 6Lo, Routing over Low Power and Lossy Networks, Application Layer Protocols: CoAP and MQTT.

**MODULE III Securing the IoT: (10 Periods)**

Security Requirements in IoT Architecture, Security in Enabling Technologies, Security Concerns in IoT Applications. Security Architecture in the Internet of Things, Security Requirements in IoT, Insufficient Authentication/Authorization, Insecure Access Control, Threats to Access Control, Privacy, and Availability, Attacks Specific to IoT. Vulnerabilities. Secrecy and Secret-Key Capacity, Authentication/Authorization for Smart Devices, Transport Encryption, Attack & Fault trees.

**MODULE IV Cloud Security for IoT: (07 Periods)**

Cloud services and IoT: offerings related to IoT from cloud service providers, Cloud IoT security controls, and an enterprise IoT cloud security architecture. New directions in cloud enabled IoT computing.

**MODULE V Applications & Case Study: (08 Periods)**

Real world design constraints, Applications, Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities, participatory sensing. Data Analytics for IoT. Software & Management Tools for IoT Cloud Storage Models & Communication APIs. Cloud for IoT: Amazon Web Services for IoT.

**Total Periods: *45***

## EXPERIENTIAL LEARNING

1. Embedded system architecture, development environment, sample applications, GPIO.
2. Sensors, interfaces, bus protocols, programming I2C devices.
3. Embedded OS, bootloader, network programming
4. Cloud programming and building a cloud service.

## RESOURCES

### TEXT BOOKS:

1. Xu, L. D., & Li, S., Securing the Internet of Things. Elsevier, 2017

2. Weippl, E., Internet of Things Security: Fundamentals, Techniques and Applications. River Publishers, 2018.

### REFERENCE BOOKS:

1. Russell, B., & Van Duren, D., Practical internet of things security. Packt Publishing Ltd, 2016.

2. Hu, F., Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press, 2016.

3. Zhou, H., The internet of things in the cloud: a middleware perspective. CRC press, 2012.

4. Hersent, O., Boswarthick, D., & Elloumi, O., The internet of things: Key applications and protocols. John Wiley & Sons, 2011.

5. Gupta, B., Agrawal, D., Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI Global, USA, ISBN13: 9781522584070, 2019.

6. Granjal, J., Monteiro, E., & Silva, J. S., Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312, 2015.

## VIDEO LECTURES:

1. Introduction to IoT, https://archive.nptel.ac.in/courses/106/105/106105166/
2. Cloud computing, http://digimat.in/nptel/courses/video/106105167/L39.html

## WEB RESOURCES:

1. https://www.coursera.org/learn/cloud-iot-platform
2. https://www.coursera.org/specializations/uiuc-iot

# PROGRAM CORE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201007-** | **ETHICAL HACKING** | 3 | - | - | - | 3 |

**Pre-Requisite**

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Course covers the technical aspects of Gain the knowledge of the use and availability of tools to support an ethical hack

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Demonstrate the knowledge on identifying, collecting and preserving digital evidence

**CO2:** Gain the knowledge of interpreting the results of a controlled attack.

**CO3:** Understand the role of politics, inherent and imposed limitations and metrics for planning of a test.

**CO4:** Comprehend the dangers associated with penetration testing.

**CO5**: To provide high end deliverables and defence planning for handling of incident management

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | - | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**MODULE – I: Introduction:** **(10 Periods)**

Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of

Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

**MODULE – II: The Business Perspective: (10 Periods)**

Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

**MODULE – III: Preparing for a Hack: (06 Periods)**

Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

**MODULE – IV: Enumeration: (09 Periods)**

Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, applications, Wardialing, Network, Services and Areas of Concern

**MODULE -V: Deliverable: (10 Periods)**

The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

**Total Periods: *45***

## EXPERIENTIAL LEARNING

**List of Excercises**

1. System Hacking
   - Extracting Administrator Passwords Using LCP
   - Hiding Files Using NTFS Streams
   - Find Hidden Files Using ADS Spy
   - Hiding Files Using the Stealth files Tool
2. Session hijacking
   - Session Hijacking Using the Zed Attack Proxy (ZAP)
   - Intercept and modify web traffic
   - Simulate a Trojan, which modifies a workstation’s proxy server settings.
3. Sniffers
   - Sniff the network
   - Analyze incoming and outgoing packets
   - Troubleshoot the network for performance
4. SQL Injection
   - Understanding when and how a web application connects to a database server in order to access data
   - Extracting basic SQL injection flaws and vulnerabilities
   - Testing web applications for blind SQL injection vulnerabilities
   - Scanning web servers and analyzing the reports

# RESOURCES

**TEXT BOOKS:**

1. James S. Tiller, "The Ethical Hack: A Framework for Business Value Penetration Testing", Auerbach Publications, CRC Press
2. EC-Council, "Ethical Hacking and Countermeasures Attack Phases", Cengage Learning

**REFERENCE BOOKS:**

1. Michael Simpson, Kent Backman, James Corley, "Hands-On Ethical Hacking and Network Defense", Cengage Learning.
2. A. Ojha, "Ethical Hacking and Cyber Security," Notion Press, 2020.

**VIDEO LECTURES:**

1. Ethical hacking, https://archive.nptel.ac.in/courses/106/105/106105217/

**WEB REOURCES:**

1. https://www.youtube.com/watch?v=K6w3c6lJmQI&ab_channel=Simplilearn
2. https://www.coursera.org/learn/ethical-hacking-essentials-ehe

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202005** | **DIGITAL FORENSICS** | 3 | - | 3 | - | 4.5 |

**Pre-Requisite** Network Forensics (22CB202004)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** Course covers the technical aspects of digital forensics including general forensic procedures, imaging, hashing, file recovery, file system basics, identifying mismatched file types, reporting, and laws regarding computer evidence. Students will also use open-source digital forensic software tools to conduct forensic examinations.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Demonstrate the knowledge on identifying, collecting and preserving digital evidence

**CO2:** Analyse the scientific principles relating to digital forensics.

**CO3:** Perform the steps included in a digital investigation from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, and the completion of legal proceedings.

**CO4:** Acquire knowledge about the Forensics methods in Digital Evidence and Data Acquisition, Duplication.

**CO5:** Apply forensic investigation on a forensic image, using various tools to recover evidence, resulting in a report documenting the investigation

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | - | - | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: Introduction (08 Periods)**

**Understanding Digital Forensics** Concepts in Digital Forensics, goals, Cybercrime, Examples in Cybercrime, Digital Forensics Categories, Digital Forensics Users, Digital Forensics Investigation Types, Readiness, Digital Evidence, Digital Forensics Examination Process, Digital Forensics Certifications.

***Essential Technical Concepts:*** File Structure, Digital File Metadata***, Timestamps Decoder (Tool),***Hash Analysis, Memory Types, Data Recovery Considerations, File Systems, Computing Environment, IP Address,

**Module 2: Acquiring Digital Evidence (07 Periods)**

Forensic Image File Format, Acquiring Volatile Memory (Live Acquisition), The Challenges of Acquiring RAM Memory, Acquiring Nonvolatile Memory (Static Acquisition), Using FTK Imager to Capture Hard Drive Hard Drive Imaging Risks and Challenges,

**Module 3: Analyzing Digital Evidence and Data Acquisition, Duplication.(10 Periods)**

Analyzing Hard Drive Forensic Images, Autopsy, Analyzing RAM Forensic Image, Capturing a RAM Memory Using Redline, Volatility Framework, Determine the best data acquisition methods, data recovery contingencies, need for data duplication, Use common data acquisition tools, Use common data duplication tools.

**Module 4: Digital Forensic Investigations (11 Periods)**

***Forensic Investigations Using EnCase:*** Understand evidence files, Verify evidence file integrity, Perform hashing, Configure EnCase, Search using EnCase, Use bookmarks in EnCase, View recovered files, Understand the master boot record, Understand the NTFS starting point, Understand hash values, Perform signature analysis, Perform e-mail recovery. Recovering Deleted Files/Folders in a FAT Partition, Recovering Files/Folders in an NTFS Partition, Hash Values, Hash Values.

**Module 5: Recovering Deleted Files and Deleted Partitions (09 Periods)**
Introduction to Recovering Deleted Files and Deleted Partitions, Tools to Recover Deleted Files, Recovering Deleted Partitions, Image File Forensics, introduction to Image Files, Steganography in Image Files, File Recovery.
***Web Browser and E-mail Forensics:*** Web Browser Forensics, E-mail Forensics, Anti forensics Techniques, Classification of Anti forensics Techniques.

**Total Periods: *45***
***Topics for self-study are provided in the lesson plan.***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1 Study of Computer Forensics and different tools used for forensic investigation.
2. How to Recover Deleted Files using Forensics Tools
3. Study the steps for hiding and extract any text file behind an imagefile/ Audio file using Command Prompt.
4. How to Extract Exchangeable image file format (EXIF) Data fromImage Files using Exifreader Software.
5. How to make the forensic image of the hard drive using EnCase Forensics.

6. How to Restoring the Evidence Image using EnCase Forensics
7. How to Collect Email Evidence in Victim PC
8. How to Extracting Browser Artifacts
9. How to View Last Activity of Your PC
10. Find Last Connected USB on your system (USB Forensics)
11. Comparison of two Files for forensics investigation by Compare IT software
12. Live Forensics Case Investigation using Autopsy

**SOFTWARE/TOOLS:**

- sleuthkit
- truecrypt
- hexedit
- autopsy
- iphoneanalyzer
- Kalilinux operating system

## RESOURCES

**TEXT BOOKS:**

1. Nihad A. Hassan, Digital Forensics Basics: A Practical Guide Using Windows OS Paperback – Feb. 26 2019.
2. Investigation Procedures and Response : EC-Council | Press

**REFERENCE BOOKS:**

1. Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI), 2nd Edition Paperback – April 19 2016 by EC-Council (Author).
2. Computer Forensics: Incident Response Essentials Paperback – Illustrated, Sept. 26 2001,by Warren G. Kruse II (Author), Jay G. Heiser (Author)

**VIDEO LECTURES:**

1. Digital Fornsics, https://www.youtube.com/playlist?list=PLsVJCLUs9YalwJGKrJj4LKpigGf9_2aZ5
2. Digital Forensics, https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-0?active-tab=description-tab

**WEB RESOURCES:**

1. https://www.coursera.org/learn/digital-forensics-concept
2. https://www.mygreatlearning.com/academy/learn-for-free/courses/cyber-forensics

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201008** | **MACHINE LEARNING FOR CYBER SECURITY** | 3 | - | - | - | 3 |

**Pre-Requisite** Advanced Computer Networks (22CB202001)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on Machine Learning concepts, quick way to detect anomalies, malware analysis and network traffic analysis by extracting used information, Examining how attackers exploit consumer-facing websites and app functionality and building machine learning based models to create a production system.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Demonstrate knowledge on cyber security and machine learning Concepts.

**CO2.** Analyze Anomaly Detection methods for building secure system.

**CO3.** Select and apply to Perform malware and Network Traffic Analysis to build robust cyber system..

**CO4.** Apply Security mechanisms for protecting consumer web.

**CO5.** Apply Machine techniques for building secured validate production system

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

## COURSE CONTENT

### Module 1: Convergence of Machine Learning and Cyber Security *(09 Periods)*

Cyber Threat Landscape, The Cyber Attacker's Economy, Overview of Machine Learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach. **Classifying and Clustering**: Training Algorithms to Learn, Supervised Classification Algorithms: Logistic Regression, Decision Trees, Decision Forests, Support Vector Machines, Naive Bayes ,k-Nearest Neighbors ,Neural Networks

### Module 2: Anomaly Detection *(07 Periods)*

**Detection**: Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection.

### Module 3 Malware Analysis and Network Traffic Analysis *(11 Periods)*

**Malware Analysis:** Understanding Malware, Feature Generation, From Features to Classification, Live malware analysis, dead malware analysis, Android Malware Analysis. **Network Traffic Analysis**: Theory of Network Defense, Machine Learning and Network Security, Building a Predictive Model to Classify Network Attacks

### Module 4 Protecting the Consumer Web *(09 Periods)*

Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Supervised Learning for Abuse Problems, Clustering Abuse.

### Module 5 Production Systems *(09 Periods)*

Defining Machine Learning System Maturity and Scalability, Data Quality, Model Quality, Performance, Maintainability, Monitoring and Alerting, Security and Reliability.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Anomaly detection using supervised learning algorithm like LOF(Local Outlier factor)
2. Study and implement intrusion detection system using SVM(Support Vector Machines)
3. Live malware analysis using unsupervised learning algorithm
4. Study and implement clustering abuse using K-Means Algorithm

## RESOURCES

### TEXT BOOKS:

1. Clarence Chio, David Freeman "Machine Learning and Security", O'Reilly Media, Inc. ISBN: 9781491979907
2. SumeetDua, Xian Du. "Data Mining and Machine Learning in Cyber security", CRC Press, ISBN:978-1439839423

**REFERENCE BOOKS:**

1. Learning Nessus for Penetration Testing, by Himanshu Kumar
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed.
3. Mastering Modern Web Penetration Testing by Prakhar Prasad

**VIDEO LECTURES:**

1. https://www.youtube.com/watch?v=cpCKhhV1wQU
2. https://www.youtube.com/watch?v=oBdB61A8Yt8

**WEB RESOURCES:**

1. Machine Learning for Cyber Security: Machine Learning and Security Protecting Systems with Data and Algorithms (Clarence Chio David Freeman) (z-lib.org)
2. https://cset.georgetown.edu/wp-content/uploads/Machine-Learning-and-Cybersecurity.pdf
3. https://www.geeksforgeeks.org/machine-learning-for-anomaly-detection/
4. https://www.malware-traffic-analysis.net/

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202006** | **DATABASE AND WEB SECURITY** | 3 | - | 3 | - | 4.5 |

**Pre-Requisite** Applied Cryptography (22CB202002)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion and hands-on experience onWeb Security Problem, Cryptographic Systems and Protocols; Privacy-Protecting Techniques, Securing Web Applications; Security models, Implementing VPDs; Secure DBMS architectures, Security mechanisms; Auditing Applications, SQL injection.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Design secure databases and communication of web applications by applying suitable tools and techniques.

**CO2.** Build Virtual Private Databases by assessing data dictionaries, policy managers and SQL server.

**CO3.** Analyze database server activities using oracle and SQL server.

**CO4.** Solve complex security problems of applications by using Preliminary analysis, requirement analysis and cryptographic protocols.

**CO5.** Defend privacy of applications by implementing privacy protection techniques.

**CO6.** Interpret ethical principles in security and privacy in the areas of web and database applications and follow in professional practice.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | 3 | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **CO6** | 3 | 3 | 3 | - | | | |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: SECURITY MODELS AND VIRTUAL PRIVATE DATABASES** ***(09 Periods)***

**Database Application Security Models:** Introduction, Types of users, Security models, Application types, Application security models.

**Virtual Private Databases:** Introduction, Overview of VPD, Implementing VPDs, Implementing Oracle VPD, Viewing VPD Policies and application context using the data dictionary and policy manager, Implementing row and column level security with SQL server.

### Module 2: DATABASE SECURITY DESIGN *(09 Periods)*

**Secure DBMS Design:** Introduction, Security mechanisms in DBMSs, Secure DBMS architectures.
**Design of Secure Databases:** Preliminary analysis, Requirement analysis and security policy selection, Conceptual design, Logical design, Physical design, Implementation of security mechanisms, Verification, and testing.

### Module 3: DATA AUDITING AND AUDITING DATABASE ACTIVITIES *(09 Periods)*

**Application Data Auditing:** Introduction, DML action auditing architecture, Oracle triggers, SQL server triggers, Fine grained auditing with Oracle, DML statement audit trail, Auditing application errors with Oracle.
**Auditing Database Activities:** Using Oracle database activities, Creating DLL triggers with Oracle, Auditing database activities with Oracle, Auditing server activity with Microsoft SQL server 2000, Implementing AQL profiler, Security auditing with SQL server, SQL injection.

### Module 4: THE WEB SECURITY *(09 Periods)*

The Web Security Problem, Risk Analysis and Best Practices, Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification.

### Module 5: THE WEB PRIVACY *(09 Periods)*

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Implement Secure coding for buffer flow heap attacks.
2. Implementation of Design methods to break authentication schemes
3. Implementation of methods for abusing Design Deficiencies against web sites
4. Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers.
5. Determine HTML injection bugs and possible measures to prevent HTML injection exploits.
6. Determine SQL injection and possible measures.
7. Creation and manipulation of database using SQL scripts and graphical interfaces.
8. Implementing DAC (Discretionary Access Control): Implementation of database security policies using DAC in oracle 10g/SQL server
9. Implementing of MAC (Mandatory Access Control) to ensure confidentiality and control information flow using either Oracle 10g or SQL server.
10. Implementation of Virtual Private Database using View using Oracle 10g or SQL server

### SOFTWARE/TOOLS:

Java (JDK 1.6 above version), SQL Server and oracle 10g

## RESOURCES

### TEXT BOOKS:

1. Hassan A. Afyouni, *Database Security and Auditing: Protecting Data Integrity and Accessibility*, Cengage Learning, 2006.
2. Simson G. Arfinkel, Gene Spafford, *Web Security, Privacy and Commerce*, O' Reilly Media, 2nd edition 2001.

### REFERENCE BOOKS:

1. Ron Ben Natan, *Implementing Database Security and Auditing, Elsevier Digital Press*, 2005.
2. S. Castano, M. Fugini, G. Martella, P. Samarati, *Database Security, Addison Wesley*, 1994.
3. Michael Gertz, SushilJajodia, *Handbook on Database security applications and trends*, Springer, 2008.
4. Bret Hartman, Donald J. Flinn, Konstantin Beznosov, Shirley Kawamoto, *Mastering Web Services Security*, John Wiley & Sons, Inc, 2003.

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=i0ruuJ8znYo
2. https://www.youtube.com/watch?v=yuPvoPAlhV4
3. https://www.youtube.com/watch?v=ADaz876BkP4
4. https://www.youtube.com/playlist?list=PL1y1iaEtjSYiiSGVlL1cHsXN_kvJOOhu-
5. https://www.youtube.com/watch?v=6wJ9wYOmIEE

### WEB RESOURCES:

1. Security Models and Virtual Private Databases - https://web.stanford.edu/dept/itss/docs/oracle/10gR2/network.102/b14266/apdvpoli.htm
2. Database Security Design - https://www.ibm.com/in-en/cloud/learn/database-security
3. Data Auditing and Auditing Database Activities- https://docs.oracle.com/cd/E18283_01/server.112/e10575/tdpsg_auditing.htm#:~:text=Auditing%20is%20the%20monitoring%20and,and%20network%20and%20multitier%20activities.
4. Web Security - https://developer.mozilla.org/en-US/docs/Web/Security
5. Web Privacy - https://ethics.csc.ncsu.edu/privacy/web/study.php

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| 22CB201009 | WIRELESS AND MOBILE NETWORK SECURITY | 3 | - | - | - | 3 |

| | |
|---|---|
| **Pre-Requisite** | Computer System Security (22CB202003) |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** This course provides a detailed discussion on wireless networks and mobile communication systems. It introduces new wireless designs, algorithms, protocols and applications.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the security issues at different levels in mobile communication.

**CO2.** Identify Threats and vulnerabilities in cellular and Wireless Networks.

**CO3.** Analyze internal and external threats for MANET applications by applying suitable protocols to provide security solutions.

**CO4.** Analyze ubiquitous & heterogeneous wireless networks security challenges and develop secure systems.

**CO5.** Understand the security challenges and attacks in mobile commerce applications.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **CO5** | 3 | - | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **-** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: SECURITY ISSUES IN MOBILE COMMUNICATION** ***(10 Periods)***

Mobile Communication History, Security-Wired vs Wireless, Security Issues and Requirements in Wireless Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application-level Security

**Security of Device, Network, and Server Levels:** Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security.

**Module 2: APPLICATION LEVEL SECURITY IN WIRELESS NETWORKS AND CELLULAR NETWORKS** ***(09 Periods)***

Application of WLANs, Wireless Threats, Some Vulnerabilities and Attack Methods over WLANs, Security for 1G & 2G Wi-Fi Applications, Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM, GPRS and UMTS security for applications, 3G security for applications.

**Module 3 APPLICATION LEVEL SECURITY IN MANETS** ***(08 Periods)***

MANETs, applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET Applications, Internal Threats for MANET Applications, Some of the Security Solutions.

**Module 4 APPLICATION LEVEL SECURITY IN UBIQUITOUS NETWORKS AND HETEROGENEOUS WIRELESS NETWORKS** ***(10 Periods)***

Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC, Security Attacks on UC Networks, Some of the Security Solutions for UC, Heterogeneous Wireless network architecture, Heterogeneous network application in disaster management, Security problems and solutions in heterogeneous wireless networks

**Module 5 SECURITY FOR MOBILE COMMERCE APPLICATION** ***(08 Periods)***

M-commerce Applications, M-commerce Initiatives, Security Challenges in Mobile E-commerce, Types of Attacks on Mobile E-commerce, A Secure M-commerce Model Based on Wireless Local Area Network, Some of M-Commerce Security Solutions.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

The following is the sample. Faculty shall frame according to the course domain.

1. Study of various Security Issues in Mobile Communication
2. Study on Security Issues and attacks in cellular networks
3. Study on Application Level Security in various networks
4. Study how to Develop an M-Commerce App and Maintain its Security

## RESOURCES

### TEXT BOOKS:

1. Pallapa Venkataram, B. Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill, 2010.

### REFERENCE BOOKS:

1. Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley, 2009.
2. Tara M. Swaminathan and Charles R. Eldon, Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002.

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=fasXvwixO4I
2. https://nptel.ac.in/courses/117102062

### WEB RESOURCES:

1. https://study.com/academy/course/computer-science-323-wireless-mobile-networking.html
2. https://www.digimat.in/nptel/courses/video/106106167/L01.html
3. https://www.coursera.org/lecture/security-awareness-training/mobile-devices-and-security-EMjmM

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202007** | **NETWORK ANOMALY DETECTION SYSTEM** | 3 | - | 3 | - | 4.5 |

| | |
|---|---|
| **Pre-Requisite** | Advanced Computer Networks (22CB202001) |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** This course provides a detailed discussion and hands-on experience on network anomalies and characterizing such anomalies and detecting them. It includes discussion on the possible vulnerabilities a network faces at various layers due to weaknesses in the protocols or other reasons. It introduces various types of layer-specific intrusions and modes of operation.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Understand the concepts of Network Anomalies and detect anomalies in network data.
**CO2**. Analyze various feature selection methods and tools used for the detection of network anomalies.
**CO3**. Analyze machine learning approaches to detect network anomalies
**CO4**. Evaluate the performance of network anomaly detection methods using appropriate metrics.
**CO5.** Demonstrate skills on Attack Launching and Network Monitoring Tools.

**CO6:** Work independently or in team to solve problems with effective communication

### CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | 3 | 3 | - | - | - | - |
| **CO6** | 3 | 2 | 2 | 2 | | | |
| **Course Correlation Mapping** | **3** | **3** | **3** | **2** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module I: ANOMALIES IN A NETWORK: (09 Periods)**

***Anomalies in a Network:*** Network Vulnerabilities, Security-Related Network Anomalies, intruder types, Precursors to an Attack, Network Attacks Taxonomy.

***Detecting Anomalies in Network Data:*** Detection of Network Anomalies, Aspects of Network Anomaly Detection, Datasets.

**Module II: FEATURE SELECTION METHODS (08 P*eriods*)**

***Feature Selection:*** Feature Selection vs. Feature Extraction, Relevance, Advantages, Applications, Prior Surveys on Feature Selection, Problem Formulation, Steps in Feature Selection

***Methods:*** Existing Methods of Feature Selection, Subset Evaluation Measures, Systems and Tools for Feature Selection.

**Module III: APPROACHES TO NETWORK ANOMALY DETECTION: (10 Periods)**

Network Anomaly Detection Methods, Types of Network Anomaly Detection Methods, Anomaly Detection Using Supervised Learning, Anomaly Detection Using Unsupervised Learning, Anomaly Detection Using Probabilistic Learning, Anomaly Detection Using Soft Computing, Knowledge in Anomaly Detection, Anomaly Detection Using Combination Learners.

**Module IV: EVALUATION METHODS (09 Periods)**

Accuracy, Performance, Completeness, Timeliness, Stability, Interoperability, Data Quality, Validity and Reliability, Alert Information, Unknown Attacks Detection, Updating References.

**Module V: TOOLS AND SYSTEMS (09 P*eriods*)**

Attacker's Motivation, Steps in Attack Launching, Launching and Detecting Attacks, Attack Related Tools, Attack Launching Tools, Network Monitoring Tools, Attack Detection Systems.

**Total Periods: *45***

***Topics for self-study are provided in the lesson plan.***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
2. Study of packet sniffer tools like wireshark. Use the tools to do the following
   a. Observer performance in promiscuous as well as non-promiscous mode.
   b. Show that packets can be traced based on different filters.
3. Download and install nmap. Use it with different options to scan open ports, perform OS Finger printing, do a ping scan, TCP port scan, UDP port scan, etc.
4. Use the Nessus tool to scan the network for vulnerabilities.
5. Implement a code to simulate various DOS attacks on the data collected in Experiment-2.
6. Install IDS (e.g. SNORT) and study the logs.

7. Implement snort over Microsoft windows in sniffer mode.
8. Build the snort rules over Linux in IDS Mode.
9. Configure the snort to work as Intrusion Prevention Systems (IPS).
10. Create firewalls using iptables in linux & Firewalls.

**SOFTWARE/TOOLS:**

- Wireshark
- Nmap
- Nessus tool
- SNORT

## RESOURCES

**TEXT BOOKS:**

1. Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita, "*Network Anomaly Detection: A Machine Learning Perspective*," CRC Press, 2014.

**REFERENCE BOOKS:**

1. Carl Endorf, Eugene Schultz and Jim Mellander, "*Intrusion Detection and Prevention*," McGraw-Hill, 2004
2. Stephen Northcutt, Judy Novak, "*Network Intrusion Detection*," New Riders Publishing, 3rd Edition, 2002
3. Karen Scarfone, Peter Mell, *Guide to Intrusion Detection and Prevention System (IDPS) National Institute of Standards and Technology*, Technology Administration, U.S. Department of Commerce, First Edition, 2007.
4. Stephen Northcutt and Judy Novak, *Network Intrusion Detection*, New Riders, Third Edition, 2003.
5. Peter Szor, *The Art of Computer Virus Research and Defense*, Symantec Press, 2005.
6. Markus Jakobsson and Zulfikar Ramzan, *Crime ware, Understanding New Attacks and Defenses*, Symantec Press, 2008.

**VIDEO LECTURES:**

1. Intrusion Detection Systems, https://www.coursera.org/lecture/detecting-cyber-attacks/intrusion-detection-systems-UeDqJ
2. Network Traffic Analysis Anomaly Detection, https://www.youtube.com/watch?app=desktop&v=gK1KwC_aGBc&ab_channel=LevelEffect

**WEB RESOURCES:**

1. https://www.youtube.com/watch?v=RYB4cG8G2xo
2. The State of the Art in Intrusion Prevention and Detection by Al-Sakib Khan Pathan - http://docshare03.docshare.tips/files/20579/205795770.pdf

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201010** | **INDUSTRIAL CRITICAL INFRASTRUCTURE SECURITY** | 3 | - | - | - | 3 |

**Pre-Requisite** Advanced Computer Networks (22CB202001)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides detailed discussion on Critical Infrastructures, Industrial Network, Control Systems Security, Industrial Network Protocols, Risk and vulnerability assessment, Threat detection and risk management

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the basic concepts of critical infrastructure, importance of securing industrial networks and defending techniques for cyber threats.

**CO2.** Analyze industrial control systems network design, architecture and safety instrumental systems.

**CO3.** Analyze various industrial network protocols and industrial cyber threats, attack trends and dealing network infection.

**CO4.** Apply appropriate methods to identify risks, assess vulnerabilities and mitigate risks

**CO5.** Implement security and access control mechanisms to avoid anomalies.

## CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** |
| **CO1** | 3 | - | - | - | - | - | - |
| **CO2** | 3 | 3 | - | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | 3 | - | - | - | - |
| **CO5** | 3 | - | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels:*** ***3: High;*** ***2: Medium;*** ***1: Low***

## COURSE CONTENT

**Module 1: Industrial Networks** ***(08 Periods)***

Common Industrial Security Recommendations, Advanced Industrial Security Recommendation, Common Misperceptions About Industrial Network Security, Importance of Securing Industrial Networks, Evolution of The Cyber Threat, Defending Against Modern Cyber Threats, Insider Threats, Hacktivism, Cyber Crime, Cyber Terrorism, And Cyber War

**Module 2: Introduction To ICS Network Design And Architecture** ***(12 Periods)***

System Assets, System Operations, Process Management, Safety Instrumented Systems, Smart Grid Operations, Network Architectures.
Common Topologies, Network Segmentation, Network Services, Wireless Networks, Remote Access, Performance Considerations, Safety Instrumented Systems.

**Module 3: Industrial Network Protocols and Threats** ***(09 Periods)***

Overview of Industrial Network Protocols, Fieldbus Protocols, Backend Protocols, AMI and the Smart Grid, Industrial Protocol Simulators, Common Industrial Targets, Common Attack Methods, Examples of Advanced Industrial Cyber Threats, Attack Trends, Dealing with an Infection.

**Module 4: Risk and Vulnerability Assessments** ***(07 Periods)***

Cyber Security and Risk Management, Methodologies for Assessing Risk within Industrial Control Systems, System Characterization, Threat Identification, Vulnerability Identification, Risk Classification and Ranking, Risk Reduction and Mitigation.

**Module 5: Security and Access Controls** ***(09 Periods)***

Identifying and Classifying Security Zones and Conduits, Network Segmentation, Implementing Network Security Controls, Implementing Host Security and Access Controls. Exception, Anomaly, and Threat Detection: Exception Reporting, Behavioral Anomaly Detection, Behavioral Whitelisting, Threat Detection

***Total Periods: 45***

## RESOURCES

### TEXT BOOKS:

1. E.D. Knapp: Industrial Network Security. Elsevier, 2011.
2. Edward J. M. Colbert, Alexander Kott: Cyber-security of SCADA and Other Industrial Control Systems. Springer International Publishing, 2016.

### REFERENCE BOOKS:

1. Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann, Handbook on Securing Cyber-Physical Critical Infrastructure, (Elsevier), 2012.
2. Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain: Cyber Security for Cyber Physical Systems. Springer International Publishing, 2018.

### VIDEO LECTURES:

1. Network and Computer Security, https://ocw.mit.edu/courses/6-857-network-and-computer-security-spring-2014/
2. Comparative Security and Sustainability, https://ocw.mit.edu/courses/17-559-comparative-security-and-sustainability-fall-2004/

### WEB RESOURCES:

1. https://www.youtube.com/watch?v=3uxt5WeVCYg

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB202008** | **NETWORK OPERATIONS AND SECURITY** | 3 | - | 3 | - | 4.5 |

**Pre-Requisite** Advanced Computer Networks (22CB202001)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This Course Provides a Detailed Discussion on host and user management. It provides the policies and methods for Configuration and maintenance of system and also network tools and methods for monitoring the performance networks and provides the authentication, Mitigation and access control for both wired and wireless networks.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1:** Apply mechanisms for Host and User management tasks

**CO2.** Apply policies and methods for system Configuration and maintenance.

**CO3.** Analyze and monitor network performance and remote file access using Network tools.

**CO4.** Apply Authentication and Access Control methods for network security

**CO5.** Apply Mitigation Techniques for Wireless Network security.

### CO-PO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| CO1 | 3 | 3 | 3 | - | - | - | - |
| CO2 | 3 | 3 | 3 | - | - | - | - |
| CO3 | 3 | 3 | - | - | - | - | - |
| CO4 | 3 | 3 | 3 | - | - | - | - |
| CO5 | 3 | 3 | 3 | - | - | - | - |
| Course Correlation Mapping | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

## COURSE CONTENT

**Module I: Host and User management (09 Periods)**

**Host Management** - Global view, local action, Physical considerations of server, Computer startup and shutdown, Configuring and personalizing workstations, Installing a Unix disk, Installation of the operating system, Software installation, Kernel customization

**User Management –** Issues, User registration, Account policy, Login environment, User support services, Controlling user resources, online user services, User well-being, Ethical conduct of administrators and users, Computer usage policy

**Module II: Configuration and maintenance** **(09 P*eriods*)**

System configuration policy, Methods: controlling causes and symptoms, Change management, Declarative languages, Policy configuration and its ethical usage, Common assumptions: clock synchronization, Human–computer job scheduling, Automation of host configuration, Preventative host maintenance, SNMP tools, Cfengine, Database configuration management

**Module III: Monitoring Network Performance and Remote Access** **(09 Periods)**

Common Reasons to Monitor Networks, SNMP Monitors, Packet Sniffers, Throughput Testing, Port Scanners, Vulnerability Scanners, Network Performance, Load, and Stress Testing, Tracking Event Logs

Remote File Access, VPNs, Site-to-Site and Client-to-Site, HTTPS/Management URL, Out-of-Band Management

**Module IV: Network Security** **(09 Periods)**

**Physical Security and Device Hardening -** Adding Physical Security to the Mix, Two-Factor and Multifactor Authentication, Secured Versus Unsecured Protocols, Additional Device Hardening

**Authentication and Access Controls -** Mandatory Access Control, Discretionary Access Control, Rule-Based Access Control, Role-Based Access Control, RADIUS and TACACS+, Kerberos Authentication, Local Authentication, Lightweight Directory Access Protocol, Using Certificates, Auditing and Logging, Multifactor Authentication Factors, Access Control

**Module V: Securing Wireless Networks and Mitigation Techniques** **(09 P*eriods*)**

**Securing Wireless Networks** - WPA, WPA2, TKIP-RC4, and CCMP-AES, Wireless Authentication and Authorization, Shared, Preshared, and Open Keys

**Mitigation Techniques** - Signature Management, Device Hardening, Change Native VLAN, Switch and Port Protection, Demilitarized Zones (Perimeter Network), VLAN Network Segmentation, Privileged User Account, File Integrity Monitoring, Role Separation, Using ACLs to Restrict Access, Honeypots and Honeynets, Penetration Testing

**Total Periods: *45***

## EXPERIENTIAL LEARNING

**LIST OF EXERCISES:**

1 Configure the following servers using cisco packet tracer
A. HTTP B. DNS C. SMTP D. FTP

2. Implement cisco router configuration command list using packet tracer
A. Change router configuration B. Enabling Password C. Set Telnet Password D. Set IP Address to cisco interface E. Enable a port interface

3. Configure SSH on cisco routers and switches using cisco packet tracer.
4. Configuring VLAN and VTP on a small network of 4 switches using Packet Tracer.
5. Building a topology with spanning tree and static routing network protocols.
6. Implement the following routing protocols using cisco packet tracer.

A. OSPF B.RIP

7. Installation of Virtual box and kali linux for SNMP Monitoring.
8. Analyze the packet/Traffic using Wireshark.
9. Identify the network vulnerabilities by scanning the network using Nmap.
10. Identify the network vulnerable ports by port scanning using Nmap.

## RESOURCES

### TEXT BOOKS:

1. Mark Burgess, "Principles of Network and System Administration", *Second Edition*, John Wiley & Sons, Ltd, 2004.
2. Donald Childers and Scott Miller, "Probability and Random Processes", Second Edition, Elsevier,2012

### REFERENCE BOOKS:

1. Jesin A, "Packet tracer network simulator", PACT Publishing, 2014.
2. Angela Orebaugh, Gilbert Ramirez, Josh Burke, Larry Pesce, Joshua Wright ,Greg Morris, "Wireshark and ethereal Network protocol and analyzer toolkit", Syngress Publishing.ing,2007.
3. Himanshu Sharma, "*Kali Linux - An Ethical Hacker's Cookbook*," Packt Publishing Limited

### VIDEO LECTURES:

1. Network and Computer Security, https://ocw.mit.edu/courses/6-857-network-and-computer-security-spring-2014/

### WEB RESOURCES:

1. https://alison.com/courses?query=networking
2. https://www.infosecinstitute.com/skills/learning-paths/comptia-network/
3. https://www.koenig-solutions.com/wireshark-network-analyst-certification-training-course
4. https://www.youtube.com/watch?v=pq3yV3qpBkw

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CB201011** | **INFORMATION WARFARE** | 3 | - | - | - | 3 |

**Pre-Requisite** Advanced Computer Networks (22CB202001)

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on the full range of competitive information operations from destroying IT equipment to subtle perception management, and from industrial espionage to marketing.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Analyze the need for Information warfare and its influence on various sectors

**CO2.** Apply Deception and Sources of threat for IT systems

**CO3.** Analyze Attacks and retaliation & Attack and defence Implications of I-War for information managers.

**CO4.** Analyze Political activists, freedom fighters, and terrorists on the Web

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | 3 | - | - | - | - | - |
| **CO2** | 3 | 3 | 3 | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: Concepts in Information Warfare** ***(09 Periods)***

Fundamentals, Data, information, and knowledge, Basic strategies used in I-War, A framework for an information attack. The surprise attack, The networked society, Some specific techniques in I-War.

**Information as an intelligence weapon**: The intelligence function, Offensive and defensive operations, The intelligence cycle, Information production for the external world, Countering detrimental information, An intelligence department.

**Module 2: Deception and Sources of threat for IT systems** ***(09Periods)***

**Deception*:*** Principles, Types of deception, Digital deception, Deception by changing presentation of data, Some principles for creating an illusion, Why lie. The surveillance society.

**Sources of threat for IT systems:** Attack, Methods of attack, Steps to reduce risks, Informal interventions

**Module 3 Attacks and retaliation and Attack and defence** ***(09 Periods)***

Source of attack, Retaliation, The scenario, Possible defence against attacks, IDS characterisation, Defeating IDS.

An I-War risk analysis model, Introduction, An overview of the I-War risk analysis model approach, System design.

**Module 4 Implications of I-War for information managers and The legal perspective of I- War1** ***(09 Periods)***

**Implications of I-War for information managers:** Setting the scene, Organisational data, Organisational knowledge, Information.

**The legal perspective of I- War1:** Introduction, International law and I-War, National law and I-War, The way ahead with international laws, Conclusions on the legal perspective of I-War

**Module 5 Political activists, freedom fighters, and terrorists on the Web** ***(09 Periods)***

**Political activists, freedom fighters, and terrorists on the Web:** Introduction, Propaganda/publicity, Fundraising, Information dissemination, Reasons why cyber terrorism will become widespread, The development of cyber terrorist groups, Social activists, Perceptual intelligence and I- War.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Information warfare in the military context is easy to comprehend. There is an enemy; the concepts of information as a weapon and target are relatively obvious. However, are the same principles applicable in the modern commercial environment? What 'enemies' do companies have?
2. The need to protect the integrity of the corporate database and its delivery and storage systems is obvious. Analyze how the concept of information warfare takes this further.
3. To operate more efficiently, DoD has been rapidly moving away from isolated and stand-alone information systems to a globally integrated information structure. In doing so, it has linked together thousands of computers with the Internet as well as

other networks, and increased its dependence on computer and network technology to do its basic functions. This raises a number of concerns. What if

These systems or large parts of them were destroyed?

They were merely made unavailable for a time period?

The information they contained was compromised?

Random parts of that information were corrupted or made unreliable?

Malicious software was introduced into these systems?

An enemy decided to exploit design flaws in the infrastructure on which we depend?

An enemy was in control of a computer system on which we used to help make critical battlefield computations?

A hostile foreign nation built all of the microelectronic components we used in an important military system?

## RESOURCES

### TEXT BOOKS:

1. Bill Hutchinson & Mat Warren, Information Warfare: Corporate attack and defence in a digital world, Reed Educational and Professional Publishing Ltd.

### REFERENCE BOOKS:

1. Daniel Ventre, Information Warfare, 2nd Edition
2. William Huthinson Information Warfare: Corporate attack and defence in a digital world

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=15mFM6IPcAY
2. https://www.youtube.com/watch?v=stBBDhhNDvE

### WEB RESOURCES:

1. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf
2. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

# PROGRAM ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| 22CB201012 | COMPUTER SECURITY AUDIT AND ASSURANCE | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on security audit and assurance.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the fundamental methods used in information system auditing process

**CO2.** Understand the role of auditor and how to prepare the auditing plan for information system auditing

**CO3.** Extract the information and plan for conducting the testing process for information system auditing.

**CO4.** Apply computer assisted audit tools for auditing process and prepare an audit document

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | | |
|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
| **CO1** | 3 | 3 | - | - | - | - | - |
| **CO2** | 3 | 3 | 3 | - | - | - | - |
| **CO3** | 3 | 3 | - | - | - | - | - |
| **CO4** | 3 | 3 | - | - | - | - | - |
| **Course Correlation Mapping** | **3** | **3** | **3** | **-** | **-** | **-** | **-** |

**Correlation Levels: 3: High; 2: Medium; 1: Low;**

## COURSE CONTENT

**Module 1: Foundation for IT Audit and Assurance** ***(09 Periods)***

3 hours Assurance Services - Need for Assurance - Characteristics of Assurance Services- Types of Assurance Services Ecommerce and Electronic Funds Transfer - Future of electronic payment system.

**Audit Process:** Audit Standards - Types of Auditors and their functions - Internal Audit Function and External Auditor. Audit Plan - Developing an Audit Schedule - Audit Budget - Preliminary Review - Audit Findings - Analysis Re-examination - Verification - Recommendations - Communication Strategy.

**Module 2: Conducting Information System Audit** ***(09Periods)***

Standards - Practices and Guidelines - Information Gathering Techniques - Vulnerability - System Security Testing - Development of Security Requirements Checklist.

**Computer Assisted Audit Tools and Techniques:** Auditor Productivity Tools - Data and Resource Management - Flowcharting Techniques - Flowcharting as an analysis tool - Developing Audit Data Flow Diagrams - Appropriateness of flowcharting techniques - Computer assisted tools for operational reviews - Web Analysis tools

**Module 3 Managing IT Audit** ***(09 Periods)***

Evaluating IT Audit Quality - Criteria for assessing the audit - Criteria for assessing the auditor - Best Practices in IT Audit Planning - IT Governance: Performance Measurement - Metrics and Management - Metric Reporting and Independent Assurance.

**Module 4 Security and Service continuity** ***(09 Periods)***

Security Standards - ISO 27002 and National Institute of Standards and Technology - Information Security Controls - Security Architecture - Information Security Policy - Information Owner Responsibilities - Third- Party Responsibilities.

**Module 5 Virtual Application Security and ERP security** ***(09 Periods)***

Intranet/Extranet Security - Identity Theft - E-Commerce Application Security as a strategic and structural problem - Planning and Control Approach to E-Commerce Security Management - Internet Security and Mobile Computing Security - ERP Data Warehouse-Data Warehouse integrity checklist - ERP-Security features of the basic component.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

- Provide management with an assessment of the effectiveness of the information security management function.
- Evaluate the scope of the information security management organization and determine whether essential security functions are being addressed effectively.

## RESOURCES

### TEXT BOOKS:

1. Information Technology Control and Audit, Fourth Edition, Sandra Senft, Frederick Gallegos, Aleksandra Davis, CRC Press, 2012.

### REFERENCE BOOKS:

1. Information System Audit and Assurance, D P Dube, V P Gulati, Tata Mc-Graw Hill, 2008
2. Micheal E.Whitman, Herbert J.Mattor, “Principles of Information Security”, Course Technology, Delmar Cengage Learning, Fourth Edition, 2012.
3. Jennifer L.Bayuk, Jason Healey, Paul Rohmeyer and Marcus Sachs, “Cyber Security Policy Guidebook”, John Wiley Sons, Kindle Edition, 2012

### VIDEO LECTURES:

1. https://www.coursera.org/learn/information-systems-audit
2. https://www.youtube.com/watch?v=hPKWSU9lMjA&ab_channel=Dr.AsadiSrinivasulu

### WEB RESOURCES:

1. https://www.youtube.com/watch?v=vedA6durg8U&ab_channel=RutgersAccountingWeb

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22AI201701** | **BUSINESS ANALYTICS** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course emphasizes on the basic concepts of Business Analytics. It covers the basic excel skills, Excel look up functions for database queries in business analytics. By the end of this course students will acquire basic knowledge to implement statistical methods for performing descriptive, predictive and prescriptive analytics.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Understand the basic concepts and models of Business Analytics

**CO2.** Select Suitable basic excel function to perform analytics on spread sheets.

**CO3.** Apply different statistical techniques and distributions for modeling the data

**CO4.** Develop user-friendly Excel applications by using statistical models for effectiveness decision making.

**CO5.** Analyze the performance of different optimization models used in prescriptive analytics on Binary and Categorical data.

## CO-PO-PSO Mapping Table:

| Course Outcomes | Program Outcomes | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 |
| CO1 | 2 | 1 | - | - | - | - | - | - | - |
| CO2 | 2 | 3 | - | - | - | - | - | - | - |
| CO3 | 2 | 2 | - | - | 3 | - | - | - | - |
| CO4 | 1 | 1 | - | - | - | - | - | - | 3 |
| CO5 | - | - | - | - | - | - | - | - | - |
| **Course Correlation Mapping** | **2** | **2** | **-** | **-** | **3** | **-** | **-** | **-** | **3** |

***Correlation Levels: 3: High; 2: Medium; 1: Low***

## COURSE CONTENT

**Module 1: FOUNDATIONS OF BUSINESS ANALYTICS** ***(9 Periods)***

Introduction, What is Business Analytics, Evolution of Business Analytics, Scope of Business Analytics, Data for Business Analytics, Applications of Business Analytics, Models in Business Analytics, Problem Solving with Analytics.

**Module 2: ANALYTICS ON SPREADSHEETS** ***(9 Periods)***

Basic Excel Skills, Excel Functions, Using Excel Lookup Functions for Database Queries, Spreadsheet Add-Ins for Business Analytics.
Visualizing and Exploring Data: Data Visualization, Creating Charts In Microsoft Excel, Other Excel Data Visualization, Statistical Methods For Summarizing Data, Exploring Data Using Pivot tables.

**Module 3: DATA MODELING** ***(9Periods)***

Basic concepts of Probability, Random Variables and Probability Distributions, Continuous Probability Distributions.
Statistical Sampling, Estimation population parameters, Sampling Error, Sampling Distributions, Hypothesis Testing, ANOVA, Chi Square Test.

**Module 4: Predictive analytics** ***(9 Periods)***

Trend lines And Regression Analysis, Modeling Relationships And Trends In Data, Simple Linear Regression, Multiple Linear Regression, Building Good Regression Models,
Strategies for predictive decision modeling, implementing models on spreadsheets, spreadsheet applications in business analytics, developing user-friendly excel applications, analysing uncertainty and model assumptions, model analysis using analytic solver platform

**Module 5: Prescriptive analytics** ***(9Periods)***

***Linear Models:*** Building Linear Models, Implementing Linear Optimization Models On Spreadsheets, Graphical Interpretation Of Linear Optimization, Linear Optimization Models for prediction and Insight.
***Integer Models***: Solving models with Integer Variables, Integer Optimization Models with Binary Numbers
***Decision Analysis***: Formulating Decision Problems, Decision Strategies Without Outcome Probabilities, Decision Trees With Outcome Probabilities, Decision Trees.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. **Diabetic Prediction:**

   The National Institute of Diabetes and Digestive and Kidney Diseases has a created a dataset. The objective of the dataset is to diagnostically predict whether or not a patient has diabetes, based on certain diagnostic measurements included in the dataset. Several constraints were placed on the selection of these instances from a larger database. In particular, all patients here are females at least 21 years old of Pima Indian heritage. The datasets consists of several medical predictor variables and one target variable, Outcome. Predictor variables includes the number of pregnancies the patient has had, their BMI, insulin level, age, and so on. Build a machine learning model to accurately predict whether or not the patients in the dataset have diabetes or not?

2. Solve the house price prediction problem using **Linear regression analysis** method. Optimize the parameters of the regression function using gradient descent method.
3. Visualize the decision tree built for solving Heart disease prediction problem and measure the impurity of nodes created via **Decision Tree Analysis**.

   Dataset:https://www.kaggle.com/arviinndn/heart-disease-prediction-uci dataset/data
4. The data set baby boom (Using R) contains data on the births of 44 children in a one- day period at a Brisbane, Australia, hospital. Compute the skew of the wt variable, which records birth weight. Is this variable reasonably symmetric or skewed?
5. Visualize the **Distribution of data** with different feature scaling methods on online news popularity dataset for article word count.

   Dataset:https://www.kaggle.com/datasets/deepakshende/onlinenewspopularity
6. **Human Activity Recognition System:**

   The human activity recognition system is a classifier model that can identify human fitness activities. To develop this system, you have to use a smart phone dataset, which contains the fitness activity of 30 people which is captured through smart phones. This system will help you to understand the solving procedure of the **Multi-classification problem**.

## RESOURCES

### TEXT BOOKS:

1. James Evans, *Business Analytics*, Pearson Education, 2nd Edition, 2017.

### REFERENCE BOOKS:

1. Marc J.Schniederjans, *Business Analytics*, Pearson Education,2015
2. Camm,Cochran, *Essentials of Business Analytics*, Cenage learning, 2015

### VIDEO LECTURES:

1. https://nptel.ac.in/courses/110105089
2. https://archive.nptel.ac.in/courses/110/107/110107092/
3. https://nptel.ac.in/courses/110106050

### WEB RESOURCES:

1. https://www.proschoolonline.com/certification-business-analytics-course/what-is-ba
2. https://michael.hahsler.net/SMU/EMIS3309/slides/Evans_Analytics2e_ppt_01.pdf
3. https://www.guru99.com/business-analyst-tutorial-course.html

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CM201701** | **COST MANAGEMENT OF ENGINEERING PROJECTS** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course will provide an understanding of the cost tools and techniques that can be used throughout a project's design and development. The students will be exposed to the methods, processes, and tools needed to conduct economic analysis, estimation of Project.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

| | |
|---|---|
| **CO1** | Understand the costing concepts and their role in decision-making. |
| **CO2** | Understand the project management concepts and their various aspects in selection. |
| **CO3** | Interpret costing concepts with project execution. |
| **CO4** | Knowledge of costing techniques in the service sector and various budgetary control techniques. |
| **CO5** | Become familiar with quantitative techniques in cost management. |

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| **CO1** | - | - | - | - | - | 2 |
| **CO2** | - | - | - | - | - | 2 |
| **CO3** | - | - | - | - | - | 2 |
| **CO4** | - | - | - | - | - | 2 |
| **CO5** | - | - | - | - | - | 2 |
| **Course Correlation Level** | - | - | - | - | - | 2 |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: INTRODUCTION TO COSTING CONCEPTS** ***(05 Periods)***

Objectives of a Costing System; Cost concepts in decision-making; Relevant cost, Differential cost, Incremental cost, and Opportunity cost; Creation of a Database for operational control.

**Module 2: INTRODUCTION TO PROJECT MANAGEMENT** ***(10 Periods)***

Project: meaning, Different types, why to manage, cost overruns centers, various stages of project execution: conception to commissioning. Project execution as conglomeration of technical and nontechnical activities, Detailed Engineering activities, Pre-project execution main clearances and documents, Project team: Role of each member, Importance Project site: Data required with significance, Project contracts

**Module 3: PROJECT EXECUTION AND COSTING CONCEPTS** ***(10 Periods)***

Project execution Project cost control, Bar charts and Network diagram, Project commissioning: mechanical and process, Cost Behavior and Profit Planning Marginal Costing; Distinction between Marginal Costing and Absorption Costing; Break-even Analysis, Cost-Volume-Profit Analysis, Various decision-making problems, Pricing strategies: Pareto Analysis, Target costing, Life Cycle Costing

**Module 4: COSTING OF SERVICE SECTOR AND BUDGETARY CONTROL** ***(10 Periods)***

Just-in-time approach, Material Requirement Planning, Enterprise Resource Planning, Activity Based Cost Management, Bench Marking; Balanced Score Card and Value-Chain Analysis, Budgetary Control: Flexible Budgets; Performance budgets; Zero-based budgets

**Module 5: QUANTITATIVE TECHNIQUES FOR COST MANAGEMENT** ***(10 Periods)***

Linear Programming, PERT/CPM, Transportation problems, Assignment problems, Learning Curve Theory.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1 Prepare a mini-project report regarding cost control techniques in manufacturing units.

2 Prepare a report on real-life engineering project case studies, especially those that faced cost overruns or successfully managed costs

3 Conduct hands-on budgeting exercises where participants are given a project scope, and they have to create detailed budgets.

## RESOURCES

### TEXT BOOKS:

1. John M. Nicholas, Herman Steyn Project Management for Engineering, Business and Technology, Taylor & Francis, 2 August 2020, ISBN: 9781000092561
2. Albert Lester ,Project Management, Planning and Control, Elsevier/Butterworth-Heinemann, 2007, ISBN: 9780750669566, 075066956X.

### REFERENCE BOOKS:

1. Charles T. Horngren et al Cost Accounting a Managerial Emphasis, Prentice Hall of India, New Delhi, 2011.
2. Ashish K. Bhattacharya, Principles & Practices of Cost Accounting A. H. Wheeler publisher, 1991.

3 Vohra N.D., Quantitative Techniques in Management, Tata McGraw Hill Book Co. Ltd, 2007

4 Robert S Kaplan Anthony A. Alkinson, Management & Cost Accounting, 2003

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=rck3MnC7OXA
2. https://www.youtube.com/watch?v=QWD1LMzStI4

### WEB RESOURCES:

1. https://www.superfastcpa.com/what-are-cost-concepts-in-decision-making
2. https://www.indeed.com/career-advice/career-development/project-cost-controls
3. https://www.geeksforgeeks.org/difference-between-pert-and-cpm/

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22CE201701** | **DISASTER MANAGEMENT** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course provides a detailed discussion on disaster prone areas in India, repercussions of disasters and hazards, disaster preparedness and management, risk assessment and disaster management.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Analyze the vulnerability of an area to natural and man-made disasters/hazards as per the guidelines to solve complex problems using appropriate techniques ensuring safety, environment and sustainability.

**CO2.** Analyze the causes and impacts of disasters using appropriate tools and techniques and suggest mitigation measures ensuring safety, environment and sustainability besides communicating effectively in graphical form.

**CO3.** Suggest the preparedness measures using appropriate tools and techniques and suggest mitigation measures ensuring safety, environment and sustainability.

**CO4.** Analyze the Risk Assessment using appropriate tools and techniques and suggest mitigation measures ensuring safety, environment and sustainability.

**CO5.** Design disaster management strategies to solve pre, during and post disaster problems using appropriate tools and techniques following the relevant guidelines and latest developments ensuring safety, environment and sustainability besides communicating effectively in graphical form.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| CO1 | - | - | - | - | - | 2 |
| CO2 | - | - | - | - | - | 2 |
| CO3 | - | - | - | - | - | 2 |
| CO4 | - | - | - | - | - | 2 |
| CO5 | - | - | - | - | - | 2 |
| Course Correlation Level | - | - | - | - | - | 2 |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: DISASTER PRONE AREAS IN INDIA** ***(09 Periods)***

**Introduction:** Disaster: Definition, Factors and Significance; Difference Between Hazard and Disaster; Natural and Manmade Disasters: Difference, Nature, Types And Magnitude. **Disaster Prone Areas:** Study Of Seismic Zones; Areas Prone To Floods And Droughts, Landslides And Avalanches; Areas Prone To Cyclonic And Coastal Hazards With Special Reference To Tsunami; Post-Disaster Diseases And Epidemics.

**Module 2: REPERCUSSIONS OF DISASTERS AND HAZARDS** ***(09 Periods)***

Economic Damage, Loss of Human and Animal Life, Destruction of Ecosystem. Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts And Famines, Landslides And Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks And Spills, Outbreaks Of Disease And Epidemics, War And Conflicts.

**Module 3: DISASTER PREPAREDNESS AND MANAGEMENT** ***(11 Periods)***

Preparedness: Monitoring Of Phenomena Triggering A Disaster Or Hazard; Evaluation Of Risk: Application Of Remote Sensing, Data From Meteorological And Other Agencies, Media Reports: Governmental And Community Preparedness.

**Module 4: RISK ASSESSMENT** ***(08 Periods)***

Disaster Risk: Concept and Elements, Disaster Risk Reduction, Global and National Disaster Risk Situation. Techniques of Risk Assessment, Global Co-Operation In Risk Assessment And Warning, People’s Participation In Risk Assessment. Strategies for Survival.

**Module 5: DISASTER MANAGEMENT** ***(08 Periods)***

Disaster management organization and methodology, Disaster management cycle, Disaster management in India – Typical cases and Cost–benefit analysis, Disaster management programs implemented by NGOs and Government of India, Usage of GIS and Remote sensing techniques in disaster management, Leadership and Coordination in Disaster management, Emerging trends in disaster management.

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Perform hazard assessment and vulnerability analysis for any nearby town/city and prepare a detailed report of possible impacts of various disasters on environment, infrastructure and development.

2. Prepare a detailed report on the causes and effects of Tsunami that was occurred in the year 2004. Also discuss various advancements in Tsunami warning systems.

3. Identify the major causes of urban floods in cities like Chennai, Hyderabad & Mumbai. Also list various mitigation strategies to reduce the impact of floods.

4. Prepare a detailed report on how various man-made activities are directly/indirectly related to the occurrence of landslides that occurred in recent days in India.

5. Visit AP State Disaster Response and Fire Services Department and record about various methods used by them in mitigating disasters and their management.

## RESOURCES

**TEXT BOOKS:**

1. Sharma V. K., *Disaster Management, Medtech Publishing, 2nd Edition, 2013*.
2. Anand S. Arya, Anup Karanth, and Ankush Agarwal, *Hazards, Disasters and Your Community: A Primer for Parliamentarians*, GOI–UNDP Disaster Risk Management Programme, Government of India, National Disaster Management Division, Ministry of Home Affairs, New Delhi, Version 1.0, 2005

**REFERENCE BOOKS:**

1. Donald Hyndman and David Hyndman, *Natural Hazards and Disasters*, Cengage Learning, USA, 5th Edition, 2015.
2. *Disaster Management in India,* A Status Report, Ministry of Home Affairs, Govt. of India, May 2011.
3. Rajendra Kumar Bhandari, *Disaster Education and Management: A Joyride for Students, Teachers, and Disaster Managers*, Springer India, 2014.
4. Singh R. B., *Natural Hazards and Disaster Management*, Rawat Publications, 2009.
5. R. Nishith, Singh AK, *Disaster Management in India: Perspectives, issues and strategies,* New Royal book Company.
6. Sahni, PardeepEt.Al. (Eds.), *Disaster Mitigation Experiences And Reflections*, Prentice Hall of India, New Delhi.
7. Goel S. L. , *Disaster Administration And Management Text And Case Studies*, Deep &Deep Publication Pvt. Ltd., New Delhi

**VIDEO LECTURES:**

1. https://nptel.ac.in/courses/105104183
2. https://www.digimat.in/nptel/courses/video/124107010/L01.html

**WEB RESOURCES:**

1. https://egyankosh.ac.in/handle/123456789/25093
2. https://www.egyankosh.ac.in/handle/123456789/25912
3. https://www.nios.ac.in/media/documents/333courseE/12.pdf
4. https://ndmindia.mha.gov.in/images/public-awareness/Primer%20for%20Parliamentarians.pdf

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22SS201701** | **VALUE EDUCATION** | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION:** This course deals with understanding the value of education and self-development, Imbibe good values in students, and making them know about the importance of character.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Demonstrate the knowledge of values and self-development

**CO2.** Analyze the importance of the cultivation of values.

**CO3.** Learn suitable aspects of personality and behavioral development

**CO4.** Function as a member and leader in multi-disciplinary teams by avoiding faulty thinking.

**CO5.** Develop character and competence for effective studies.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** |
| **CO1** | - | - | - | - | - | 2 |
| **CO2** | - | - | - | - | - | 2 |
| **CO3** | - | - | - | - | - | 2 |
| **CO4** | - | - | - | - | - | 2 |
| **CO5** | - | - | - | - | - | 2 |
| **Course Correlation Level** | - | - | - | - | - | 2 |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

**Module 1: VALUES AND SELF-DEVELOPMENT** ***(09 Periods)***

Values and self-development –Social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non-moral valuation. Standards and principles. Value judgements- Case studies

**Module 2: IMPORTANCE OF CULTIVATION OF VALUES.** ***(09 Periods)***

Importance of cultivation of values. Sense of duty. Devotion, Self-reliance. Confidence, Concentration. Truthfulness, Cleanliness. Honesty, Humanity. Power of faith, National Unity. Patriotism. Love for nature, Discipline- Case studies

**Module 3: PERSONALITY AND BEHAVIOR DEVELOPMENT** ***(09 Periods)***

Personality and Behavior Development - Soul and Scientific attitude. Positive Thinking. Integrity and discipline, Punctuality, Love and Kindness - Case studies

**Module 4: AVOID FAULTY THINKING.** ***(09 Periods)***

Avoid fault Thinking. Free from anger, Dignity of labour. Universal brotherhood and religious tolerance. True friendship. Happiness Vs suffering, love for truth. Aware of self-destructive habits. Association and Cooperation. Doing best for saving nature - Case studies

**Module 5: CHARACTER AND COMPETENCE** ***(09 Periods)***

Character and Competence –Holy books vs Blind faith. Self-management and Good health. Science of reincarnation, Equality, Nonviolence, Humility, Role of Women. All religions and the same message. Mind your Mind, Self-control. Honesty, Studying effectively- Case studies

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. Demonstrate orally using your experiences of what values are naturally acceptable in a relationship to nurture or exploit others.
2. Prepare a report by identifying and analyzing the importance of cultivation of values.
3. Present a poster on different attitudes and behaviors.
4. Students give a PowerPoint presentation on doing best for nature.
5. Students are encouraged to bring a daily newspaper to class or to access any news related to the need for human values and note down the points.
6. Prepare a case study on how to maintain harmony with different religious people through character and competence.

(It’s an indicative one. The Course Instructor may change the activities and the same shall be reflected in the Course Handout)

## RESOURCES

### TEXTBOOKS:

1. R. Subramanaian, *Professional Ethics*, Oxford Higher Education, 2013.
2. Mike W. Martin and Roland Schinzinger, *Ethics in Engineering*, Tata McGraw-Hill, 3rd Edition, 2007.
3. Chakravarthy, S.K.: Values and ethics for Organizations: Theory and Practice, Oxford University Press, NewDelhi, 1999.

### REFERENCE BOOKS:

1. M.G. Chitakra: Education and Human Values, A.P.H. Publishing Corporation, New Delhi, 2003
2. Awakening Indians to India, Chinmayananda Mission, 2003
3. Satchidananda, M.K.: Ethics, Education, Indian Unity and Culture, Ajantha Publications, Delhi, 1991

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=90VQPZURN5c
2. https://www.youtube.com/watch?v=6ofPcK0uDaA
3. https://www.youtube.com/watch?v=5_f-7zCi79A
4. https://www.youtube.com/watch?v=2ve49BWAJRE
5. https://www.youtube.com/watch?v=kCOIfnxxQ5U

### WEB RESOURCES:

1. https://www.livingvalues.net/
2. https://livingvalues.net/materials-for-schools/
3. https://www.edb.gov.hk/en/curriculum-development/4-key-tasks/moral-civic/index.html

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| **22SS201702** | **PEDAGOGY STUDIES** | 3 | - | - | - | 3 |

| | |
|---|---|
| **Pre-Requisite** | - |
| **Anti-Requisite** | - |
| **Co-Requisite** | - |

**COURSE DESCRIPTION:** This course deals with understanding pedagogical practices that are being used by teachers in formal and informal classrooms, the effectiveness of pedagogical practices, teacher education (curriculum and practicum), and the school curriculum and guidance materials that can best support effective pedagogy.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

| | |
|---|---|
| **CO1** | Demonstrate knowledge of pedagogical methodology |
| **CO2** | Analyze the functional knowledge in Pedagogical practices, Curriculum, and Teacher Education |
| **CO3** | Learn effective pedagogical practices and apply strategies. |
| **CO4** | Function effectively as an individual and as a member of the Professional development. |
| **CO5** | Understand research Gaps and provide future Directions. |

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| CO1 | - | - | - | - | - | 2 |
| CO2 | - | - | - | - | - | 2 |
| CO3 | - | - | - | - | - | 2 |
| CO4 | - | - | - | - | - | 2 |
| CO5 | - | - | - | - | - | 2 |
| Course Correlation Level | - | - | - | - | - | 2 |

**Correlation Levels:** **3: High;** **2: Medium;** **1: Low**

## COURSE CONTENT

**Module 1: INTRODUCTION AND METHODOLOGY** ***(09 Periods)***

Aims and rationale, Policy background, Conceptual framework and terminology Theories of learning, Curriculum, Teacher education. Conceptual framework, Research questions. Overview of Methodology and Searching- Case studies

**Module 2: THEMATIC OVERVIEW** ***(09 Periods)***

Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries. Curriculum, Teacher Education- Case studies

**Module 3: EFFECTIVENESS OF PEDAGOGICAL PRACTICES** ***(09 Periods)***

Evidence on the effectiveness of pedagogical practices, Methodology for the in-depth stage: quality assessment of included studies, teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy, Theory of change, Strength and nature of the body of evidence for effective pedagogical practices. Pedagogic theory and pedagogical approaches. Teachers' Attitudes and beliefs and Pedagogic strategies- Case studies

**Module 4: PROFESSIONAL DEVELOPMENT** ***(09 Periods)***

Alignment with classroom practices and follow-up support, Peer support, and Support from the head teacher and the community. Curriculum and assessment, Barriers to learning: limited resources and large class sizes- Case studies

**Module 5: RESEARCH GAPS AND FUTURE DIRECTIONS** ***(09 Periods)***

Research design, Contexts, Pedagogy, Teacher Education, Curriculum and Assessment, Dissemination and research impact- Case studies

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. List out the self-improvement in you after going through pedagogical methodologies.
2. Discuss different practices that you would like to adopt in the curriculum.
3. Describe in your own words how you can bring effectiveness to the curriculum.
4. Imagine you are a head teacher and illustrate different barriers to learning.
5. Assume you are a teacher and Interpret different directions that you would bring for the assessment of the students.

(It's an indicative one. The Course Instructor may change the activities and the same shall be reflected in the Course Handout)

## RESOURCES

### TEXTBOOK:

1. Ackers J, Hardman F (2001) Classroom interaction in Kenyan primary schools, Compare, 31 (2): 245-261.
2. Alexander RJ (2001) Culture and pedagogy: International comparisons in primary education.

## REFERENCES:

1. Akyeampong K (2003) Teacher training in Ghana - does it count? Multi-site teacher education
2. Agrawal M (2004) Curricular reform in schools: The importance of evaluation, Journal of Curriculum Studies, 36 (3): 361-379.Oxford and Boston: Blackwell.
3. Akyeampong K, Lussier K, Pryor J, Westbrook J (2013) Improving teaching and learning of basic maths and reading in Africa: Does teacher preparation count? International Journal Educational Development, 33 (3): 272–282.
4. Chavan M (2003) Read India: A mass scale, rapid, 'learning to read' campaign.

## VIDEO LECTURES:

1. https://www.youtube.com/watch?v=WL40UeySag4
2. https://www.youtube.com/watch?v=MMXaXDIHFJ8
3. https://www.youtube.com/watch?v=7uJL1R6M4Iw

## WEB RESOURCES:

1. https://acrl.ala.org/IS/instruction-tools-resources-2/pedagogy/a-selected-list-of-journals-on-teaching-learning/
2. https://guides.douglascollege.ca/TLonline/resourcesforonlinepedagogy
3. https://www.refseek.com/directory/teacher_resources.html

# UNIVERSITY ELECTIVE

| Course Code | Course Title | L | T | P | S | C |
|---|---|---|---|---|---|---|
| 22LG201701 | PERSONALITY DEVELOPMENT THROUGH LIFE ENLIGHTENMENT SKILLS | 3 | - | - | - | 3 |

**Pre-Requisite** -

**Anti-Requisite** -

**Co-Requisite** -

**COURSE DESCRIPTION**: This course gives awareness to students about the various dynamics of personality development.

**COURSE OUTCOMES:** After successful completion of the course, students will be able to:

**CO1.** Demonstrate knowledge in Self-Management and Planning Career

**CO2.** Analyze the functional knowledge in attitudes and thinking strategies

**CO3.** Learn and apply soft skills for professional success.

**CO4.** Function effectively as an individual and as a member in diverse teams

**CO5**. Communicate effectively in public speaking in formal and informal situations.

**CO-PO Mapping Table:**

| Course Outcomes | Program Outcomes | | | | | |
|---|---|---|---|---|---|---|
| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 |
| CO1 | - | - | - | - | - | 2 |
| CO2 | - | - | - | - | - | 2 |
| CO3 | - | - | - | - | - | 2 |
| CO4 | - | - | - | - | - | 2 |
| CO5 | - | - | - | - | - | 2 |
| Course Correlation Level | - | - | - | - | - | 2 |

**Correlation Levels: 3: High; 2: Medium; 1: Low**

## COURSE CONTENT

### Module 1: SELF-ESTEEM & SELF-IMPROVEMENT *(09 Periods)*

Know Yourself – Accept Yourself; Self-Improvement: Plan to Improve - Actively Working to Improve Yourself- Exercises- case studies

### Module 2: DEVELOPING POSITIVE ATTITUDES *(09 Periods)*

How Attitudes Develop – Attitudes are Catching – Improve Your Attitudes – Exercises- case studies

### Module 3 SELF-MOTIVATION & SELF-MANAGEMENT *(09 Periods)*

Show Initiative – Be Responsible Self-Management; Efficient Work Habits – Stress Management – Employers Want People Who can Think – Thinking Strategies- Exercises- case studies

### Module 4 GETTING ALONG WITH THE SUPERVISOR *(09 Periods)*

Know your Supervisor – Communicating with your Supervisor – Special Communication with your Supervisor – What Should you Expect of Your Supervisor? – What your Supervisor expects of you - Moving Ahead Getting Along with your Supervisor- Exercises- case studies

### Module 5 WORKPLACE SUCCESS *(09 Periods)*

First Day on the Job – Keeping Your Job – Planning Your Career – Moving Ahead- Exercises- case studies

***Total Periods: 45***

## EXPERIENTIAL LEARNING

1. List out the self-improvements in you on the charts and explain in detail.
2. Discuss different famous personalities and their attitudes.
3. Describe different personalities with respect to self-motivation and self-management.
4. Imagine you are a supervisor and illustrate different special communications.
5. Assume and Interpret different experiences on the first day of your job.

## RESOURCES

### TEXTBOOK:

1 Harold R. Wallace and L. Ann Masters, Personal Development for Life and Work, Cengage Learning, Delhi, 10th edition Indian Reprint, 2011. (6th Indian Reprint 2015)

2 Barun K. Mitra, Personality Development and Soft Skills, Oxford University Press, 2011.

### REFERENCE BOOKS:

1. K. Alex, Soft Skills, S. Chand & Company Ltd, New Delhi, 2nd Revised Edition, 2011.
2. Stephen P. Robbins and Timothy A. Judge, Organizational Behaviour, Prentice Hall, Delhi, 16th edition, 2014

### VIDEO LECTURES:

1. https://www.youtube.com/watch?v=6Y5VWBLi1es
2. https://www.youtube.com/watch?v=H9qA3inVMrA

### WEB RESOURCES:

1. https://www.universalclass.com/.../the-process-of-perso...
2. https://www.ncbi.nlm.nih.gov/pubmed/25545842
3. https://www.youtube.com/watch?v=Tuw8hxrFBH8